

# NAVAL POSTGRADUATE SCHOOL

## Monterey, California



### THESIS

**DEVELOPING CORE COMPETENCIES AND  
MEASURES OF EFFECTIVENESS FOR A NAVY  
MEDICAL CHIEF INFORMATION OFFICER**

by

Thomas E. Moszkowicz

September, 1997

Thesis Advisor:  
Associate Advisor:

Barry Frew  
Mark Nissen

Approved for public release; distribution is unlimited.

19980311 117

# REPORT DOCUMENTATION PAGE

Form Approved  
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE  
September 1997

3. REPORT TYPE AND DATES COVERED  
Master's Thesis

4. TITLE AND SUBTITLE : DEVELOPING CORE COMPETENCIES AND MEASURES OF EFFECTIVENESS FOR A NAVY MEDICAL CHIEF INFORMATION OFFICER

5. FUNDING NUMBERS

6. AUTHOR(S)

Moszkowicz, Thomas E.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Postgraduate School  
Monterey, CA 93943-5000

8. PERFORMING  
ORGANIZATION REPORT  
NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSORING /  
MONITORING  
AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

While not all organizations benefit from the establishment of a Chief Information Officer (CIO), organizations that rely on information resources to accomplish their mission will gain a definite strategic advantage from developing an executive level position that can deal strategically with information technology and information resources. The Department Of the Navy (DON) medical department has established the position of CIO in a number of locations throughout the world. The purpose of this thesis is to use critical success factors to identify core competencies and skills essential for civilian medical CIOs and the core competencies and skills identified as essential for Department of Defense CIOs. By combining these two groups of core competencies and skills, this thesis develops a set of core competencies and skills necessary for a DON medical department CIO. Additionally this thesis develops measures of effectiveness for the medical CIO in a DON environment to gauge his effectiveness in contributing to the executive management of the organization.

14. SUBJECT TERMS

Chief Information Officer, Critical Success Factors, Core Competency

15. NUMBER OF  
PAGES

160

16. PRICE CODE

17. SECURITY CLASSIFICATION  
OF REPORT

Unclassified

18. SECURITY CLASSIFICATION  
OF THIS PAGE

Unclassified

19. SECURITY CLASSIFICATION  
OF ABSTRACT

Unclassified

20. LIMITATION  
OF ABSTRACT

UL



Approved for public release; distribution is unlimited

**DEVELOPING CORE COMPETENCIES AND MEASURES OF  
EFFECTIVENESS FOR A NAVY MEDICAL CHIEF INFORMATION OFFICER**

Thomas E. Moszkowicz  
Lieutenant Commander, United States Navy Reserve  
B.S. Pharmacy, University of Toledo, 1975

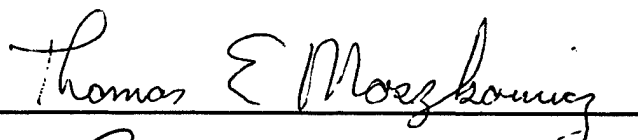
Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT**

from the

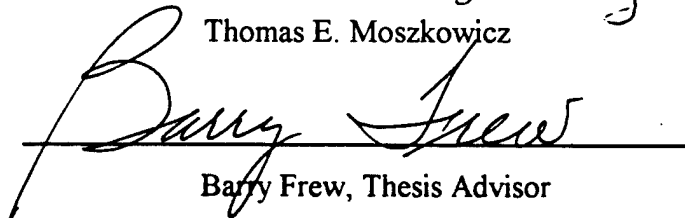
**NAVAL POSTGRADUATE SCHOOL  
September, 1997**

Author:

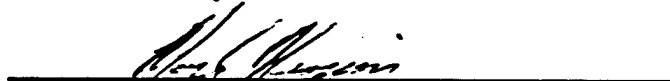


Thomas E. Moszkowicz

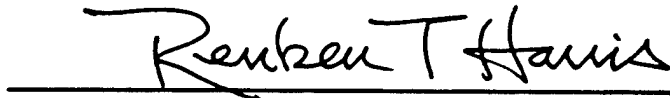
Approved by:



Barry Frew, Thesis Advisor



Mark Nissen, Associate Advisor



Reuben T. Harris, Chairman  
Department of Systems Management



## **ABSTRACT**

While not all organizations benefit from the establishment of a Chief Information Officer (CIO), organizations that rely on information resources to accomplish their mission will gain a definite strategic advantage from developing an executive level position that can deal strategically with information technology and information resources. The Department Of the Navy (DON) medical department has established the position of CIO in a number of locations throughout the world. The purpose of this thesis is to use critical success factors to identify core competencies and skills essential for civilian medical CIOs and the core competencies and skills identified as essential for Department of Defense CIOs. By combining these two groups of core competencies and skills, this thesis develops a set of core competencies and skills necessary for a DON medical department CIO. Additionally this thesis develops measures of effectiveness for the medical CIO in a DON environment to gauge his effectiveness in contributing to the executive management of the organization.



## TABLE OF CONTENTS

I. INTRODUCTION .....	1
A. GENERAL OVERVIEW .....	1
B. PURPOSE .....	2
C. RESEARCH QUESTIONS .....	2
II. BACKGROUND .....	5
A. OVERVIEW OF MEDICAL CHIEF INFORMATION OFFICER IN A CIVILIAN SETTING .....	5
1. History of the Title of Chief Information Officer .....	5
2. Current Environment of Civilian Medical CIO .....	9
a. Inter-Organizational Forces .....	9
b. Extra-Organizational Forces .....	15
3. Professional Organizations and Credentialing .....	18
B. OVERVIEW OF CHIEF INFORMATION OFFICER IN A DEPARTMENT OF DEFENSE SETTING .....	19
1. Introduction .....	19
2. ITMRA Mandate .....	21
a. Background .....	21
b. Chief Information Officer and Chief Information Officer Council .....	22
c. Capital Planning and Performance Based Management .....	24
d. Modular Contracting and Purchasing .....	27
e. Competition .....	28
f. Information Technology Resources Board .....	29
g. Government Information Technology Services Board .....	30
3. Credentialing of DOD CIOs .....	31
III. METHODOLOGY .....	33
A. DISCUSSION OF CRITICAL SUCCESS FACTORS .....	33
1. Introduction .....	33
2. The Structure of the Industry .....	33
3. The Company or Organization .....	34
4. The Environment .....	34
5. Temporal Factors .....	35
B. DISCUSSION OF SURVEY METHODOLOGY .....	35



C. DISCUSSION OF THESIS METHODOLOGY .....	37
IV. FINDINGS .....	39
A. RESPONSIBILITIES OF CIVILIAN MEDICAL CHIEF INFORMATION OFFICER.....	39
1. Introduction .....	39
2. Aligning the Information Systems Function and Activities with the Organization's Strategies.....	40
3. Strengthening the Role of Chief Information Officer .....	43
4. Creation, Alteration and Management of the Composition and Characteristics of the Information Technology Asset .....	46
5. Making Clinical Information Systems More Useful and Relevant to Clinicians .....	48
6. Facilitate the Transition to the Integrated Delivery Network .....	51
7. Developing Methods to Handle Security, Privacy and Confidentiality Concerns. ....	52
B. CORE COMPETENCIES OF A CIVILIAN MEDICAL CHIEF INFORMATION OFFICER.....	57
1. Introduction .....	57
2. Technological Competence.....	57
3. Health Care Business Competence.....	59
4. Management Competence.....	61
5. Leadership Competence.....	63
6. Systems Thinking Competence .....	64
7. Communications Competence.....	66
8. Change Management Competence .....	67
C. RESPONSIBILITIES OF A DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER.....	68
1. Introduction .....	68
2. Develop and Sell a Strategic Plan .....	70
3. Implement an Information Technology Architecture that Supports the Strategic Plan .....	72
4. Set Goals for Information Technology Within the Department of the Navy .....	75
5. Manage and Establish Credibility for Information Resource Management Within Department of the Navy .....	76
6. Increase the Technological Maturity of the Department of the Navy .....	76
7. Participate in and Guide the Chief Information Officer Council .....	77

<b>D. CORE COMPETENCIES OF A DEPARTMENT OF DEFENSE</b>	
<b>CHIEF INFORMATION OFFICER.....</b>	<b>78</b>
1. Introduction .....	78
2. Political Competence .....	78
3. DOD Business Competency .....	80
4. Communications Competence.....	81
5. Management Competence.....	82
6. Technological Competence.....	83
7. Leadership Competence.....	84
8. Change Management Competence .....	84
<b>E. SURVEY OF NAVY MEDICAL CHIEF INFORMATION</b>	
<b>OFFICERS .....</b>	<b>85</b>
1. Introduction .....	85
2. Demographics .....	86
3. Determining if Respondent is a Chief Information Officer .....	86
4. Core Competencies .....	90
<b>F. CORE COMPETENCIES OF A NAVY MEDICAL CHIEF</b>	
<b>INFORMATION OFFICER.....</b>	<b>91</b>
1. Introduction .....	91
2. Leadership Competence.....	94
3. Communication Competence .....	95
4. Technological Competence.....	96
5. Management Competence.....	97
6. Change Management Competence .....	99
7. DOD Health Care Business Competence .....	99
8. Political Competence .....	100
9. Systems Thinking Competence .....	101
<b>G. SKILLS NEEDED BY A NAVY MEDICAL CHIEF INFORMATION</b>	
<b>OFFICER.....</b>	<b>102</b>
<b>H. MEASURES OF EFFECTIVENESS OF NAVY MEDICAL CHIEF</b>	
<b>INFORMATION OFFICER.....</b>	<b>104</b>
1. Current Measures of Effectiveness for Navy Medical Chief	
Information Officers .....	104
2. Measures of Effectiveness of Civilian Medical Chief Information	
Officers .....	106
3. Potential Measures of Effectiveness of a Navy Medical Chief	
Information Officer .....	108
a. Introduction .....	108
b. Leadership Competence Measures of Effectiveness .....	109

c. Communication Competence Measures of Effectiveness .....	110
d. Technological Competence Measures of Effectiveness .....	111
e. Management Competence Measures of Effectiveness .....	111
f. Change Management and Systems Thinking Measures of Effectiveness.....	113
g. Department of Defense Health Care Business Competence Measures of Effectiveness.....	113
h. Political Competence Measures of Effectiveness.....	114
4. Use of Measures of Effectiveness of a Navy Medical Chief Information Officer .....	114
V. CONCLUSIONS AND RECOMMENDATIONS.....	115
A. CRITICAL SUCCESS FACTORS AND CORE COMPETENCIES .....	115
B. MEASURES OF EFFECTIVENESS .....	117
C. RECOMMENDATIONS .....	119
1. Navy Medical Department Recommendation .....	119
2. Educational Program Recommendation .....	121
APPENDIX A. STEPS FOR MEASURING DOD IT PERFORMANCE .....	123
APPENDIX B. NAVY MEDICAL CHIEF INFORMATION OFFICER SURVEY.....	125
APPENDIX C. INDIVIDUAL RESULTS OF THE NAVY MEDICAL CHIEF INFORMATION OFFICER SURVEY .....	129
APPENDIX D. PERCENTAGE OF RESPONDENTS WHO SELECTED EACH TOPIC AS A CORE COMPETENCY .....	133
APPENDIX E. SENGE'S LAWS OF THE FIFTH DISCIPLINE.....	135
LIST OF REFERENCES .....	137
INITIAL DISTRIBUTION LIST .....	143

## LIST OF FIGURES

1. Patient Flow Scenario in the Continuum of Care.....	11
2. Component Alignment Model.....	42
3. Technology / Reporting Level Matrix.....	87
4. Formation of Navy medical CIO's Core Competencies.....	94



## **LIST OF TABLES**

1. Summary of Technologies in IS Security Management.....	55
2. Relation of Disclosure Threats to Security Technologies.....	56
3. CIO's Responsibility for Technology Management.....	89



## ACKNOWLEDGMENT

The author would like to extend his thanks and appreciation to a number of people for their assistance in making his thesis a valuable learning experience. Thanks go to the staff of the Dudley Know Library for all of their help in providing the tools necessary to conduct literature search for this thesis. Thanks are extended to Captain James Scaramozzino, from the Institute for Defense Education and Analysis, Naval Postgraduate School Monterey, California, who provided funding for the author to attend the Navy medical CIO Conference/College of Healthcare Information Managers "Information Management Executive Course," in June of 1997. The survey and interviews conducted at this conference provide the author with data to validate his work and invaluable reference material. Thanks are also extended thesis advisor Professor Barry Frew, whose patience and wisdom lead to a successful completion of this project and to associate advisor Dr. Mark Nissen for his keen insight in providing fine tuning of the thesis. Finally, deep, heartfelt and special thanks are extended to my wife Cathy and sons Ben and Adam. Ben, thank you for reading every page for grammar and content. I could not have finished without you. Adam, thank you for keeping me young at heart. Cathy, thank you for providing your love and understanding on a daily basis, sacrificing your needs to follow me around the world to allow me to meet mine, and providing peace in my life.



## **I. INTRODUCTION**

### **A. GENERAL OVERVIEW**

Dr. Marvin Langston, the Department of the Navy's (DON) Chief Information Officer (CIO), has recently stated that he favors the creation of CIO positions at the command level (Langston, 1997a). The DON medical department has established the position of CIO in a number of locations throughout the world. CIO positions have been established at hospital commands, Tricare regional offices, and as consultants to four Commander In Chief (CINC) Surgeon's staffs and three Marine Expeditionary Force (MEF) Surgeon's staffs. While not all organizations benefit from the establishment of a CIO, organizations that rely on information resources to accomplish their mission will gain a definite strategic advantage from developing an executive level position that can deal strategically with information technology (IT) and information resources (Burbridge, 1994).

The world of medicine is virtually exploding with new and expanding technologies that are revolutionizing the delivery of health care. The United States Navy is one of the largest users of information technology on the face of the earth. The rate of change in IT will accelerate as IT continues to evolve at a rate unsurpassed by any other technological change in recorded history (Hoffman 1994). Since the DON medical department lives in both worlds, the DON medical department is truly the quintessential organization that should benefit from a CIO who is properly positioned in the organization and who has the

core competencies and skills traits needed to be successful. Currently these core competencies and skills have not been defined in the DON medical environment.

## **B. PURPOSE**

The purpose of this thesis is to use critical success factors to identify the core competencies and skills essential for civilian medical CIOs and the core competencies and skills identified as essential for Department of Defense (DOD) CIOs. By combining these two groups of core competencies and skills, this thesis develops a set of core competencies and skills necessary for a DON medical department CIO. Additionally this thesis develops measures of effectiveness (MOEs) for the medical CIO in a DON environment to gauge his effectiveness in contributing to the executive management of the organization.

## **C. RESEARCH QUESTIONS**

The primary research questions this thesis answers include:

- What are the responsibilities of a medical CIO in a civilian environment?
- What are the core competencies of a medical CIO in a civilian environment?
- What are the responsibilities of a CIO in the Department of the Navy (DON) environment?
- What are the core competencies of a CIO in the DON environment?
- What similarities and differences exist between a medical CIO in a civilian environment and a CIO in a DON environment?

- What are the core competencies required of a medical CIO in a DON environment?
- Based on the core competencies required, what are the skills that a medical CIO in a DON environment should have to be an effective management executive?
- What are measures of effectiveness (MOEs) the medical CIO in a DON environment can use to determine how well he is contributing to the executive management of the organization?



## **II. BACKGROUND**

### **A. OVERVIEW OF MEDICAL CHIEF INFORMATION OFFICER IN A CIVILIAN SETTING**

#### **1. History of the Title of Chief Information Officer**

To understand the current environment in which top medical information system executives live, it is helpful to review the development of information technology (IT), information systems (ISs) and their management. ISs in the 1950's and early 1960's were operational systems that grew from automating existing processes. The change from a manual to a computer system was technical and affected few people. The four major areas of specialization were in business computing, telecommunications, specialized office products and general office products (Sprague, 1993). There were few clinical ISs. Because various technologies were developed in a fragmented and independent manner, most hospital IS departments were managed by individuals with technical backgrounds called data processing managers (DPMs), who had often started within their organization as in-house programmers. Centralized batch processing was predominant and DPMs focused on achieving machine efficiency and managing data in this centralized environment. Discussions involving data centered on file management and organization techniques for files that served individual applications. Since early computers were very sensitive to the environment and access to the equipment was limited, ISs were usually in

an area that was physically isolated from the rest of the hospital. Hence DPMs were usually isolated from the users of the systems they managed.

Things began to change in the mid-1970's. Organizations faced rising energy costs and double-digit inflation. Processing slowly began to move out of a centralized site as smaller machines came to market and users bought their own departmental word processors and mini-computers. Hospital computer users began to move from developing their own software to buying vendor provided software and hardware (Dowling, 1989). Users became involved in at least the early stages of software development. Data discussions moved to file management systems for managing corporate data files and then to the technical solution of database management systems. Health care organizations (HCOs) began to leverage the advantages of different departments sharing data for clinical and business reasons and interest in data networks grew. Faced with rising costs and users' desires for increased use of IS, a need for managerial control of information systems arose (Laudon, 1995). The former "basement" computer department became the supplier of a new vital corporate resource, information, and its leader the management information systems (MIS) director.

The 1980's saw the advent of microcomputers and accelerated the purchase of stand alone systems by hospital departmental users. This led to departmentally optimized acquisition decisions in which a pharmacy system was procured from one vendor while a laboratory system was procured from a second vendor. At the same time a patient scheduling system was procured from a third vendor. Frequently, each of these systems

operated on a different platform and was not able to be functionally integrated. The lack of an enterprise-wide technology and the focus of available applications on internal operating procedures led many health care organizations to view their IS operations as an operating expense. Not surprisingly the MIS director reported to the organization's senior financial executive. The 1980's also brought improved communication technology and continued interest in the strategic advantages that interorganizational information systems can provide. The term "information technology" now included both computers and communications.

In the 1990's microcomputers are "faster and contain more memory than the centralized mainframes of just a few years ago." (Sprague, 1993) The growth of the internet, web-based technologies, improved routing technologies, the explosion of local area networks (LANS), wide area networks (WANS) and geographic area networks (GANS) all combine to create the same type of computer connectivity among information workers that telephone connectivity provides in voice communication. While the 1960's was the era of data processing and data management, the 1970's the era of information and IS management, the 1980's and 1990's are the era of knowledge management.

Knowledge management has become arguably many corporations' greatest strategic asset. One way to measure the strategic value of knowledge, information and IT is to examine an industry's service and product delivery process. If knowledge, information and IT are the major or only inputs and outputs of the industry's service and product process, then the knowledge, information and IT are of strategic significance to

that industry (Boyle, 1993). By this measure, knowledge, information and IT are definitely strategic assets to the health care industry.

Health care is an information intensive industry and there are very strong public and private sector pressures to increase the effectiveness and efficiency of health care delivery using ISs. Drucker uses the example of the hospital as a representation of what he calls the information-based organization when he describes his vision of the typical large business around the year 2010. He writes that "the typical business will be knowledge-based, an organization composed largely of specialists who direct and discipline their own performance through organized feedback from colleagues, customers and headquarters." (Drucker, 1988) IT has taken on a strategic role in health care delivery, helping to enlarge the scope of business through a combination of technology push, which enables an organization to do things it could not formerly do, and competitive pull. In health care strategy alignment, it becomes necessary to align the four areas of IT infrastructure and processes, the organization's infrastructure and processes, the business strategy and the IT strategy. (Martin, 1997)

The recognition of the strategic value of information in the health care industry led to the development of new responsibilities for the senior IS executive. These responsibilities also led to a new title of Chief Information Officer, which first appeared in the literature in 1981 (Frenzel, 1992). The original proponents of the CIO role argued that the CIO would take a position in the executive board room equal in power and stature to the Chief Financial Officer (CFO) who many MIS directors reported to previously



(Strassman, 1994). The CIO role can be compared to the CFO role. Every executive must have some financial knowledge. It is not the CFO's responsibility to perform every financial transaction for the HCO. Rather the CFO is accountable for assuring that the financial assets of the HCO are managed appropriately (Hammer, 1996). The CIO has the same responsibility for ISs, IT, and information resources. The CIO is accountable for assuring that the ISs, IT, and information resource assets of the HCO are managed appropriately.

## **2. Current Environment of Civilian Medical CIO**

### ***a. Inter-Organizational Forces***

Until the advent of Managed Care, health care in the United States was characterized as a product of mass production. It consisted of narrow specialties, extensive departmentalization, complex dysfunctional systems and a lack of cooperation and teamwork among its members. Whether working in clinics, private offices or hospitals, health care workers typically went about their business in an "ad hoc fashion that relies on oral history rather than bonafide studies of efficiency." (Appleby, 1997) This resulted in high costs, fragmented delivery of services, compounded and fragmented care and what has been characterized as a misalignment between the hospital and the physician. Because the physician acted as an independent contractor who brought in revenue to the hospital via his patients, the physician was looked upon as a supreme being. The doctor was not questioned or required to do anything for the good of the hospital organization

that he did not want to do. In the fee for service era, the only way for the hospital organization to secure payment was to admit the patient and charge for each service rendered. This is referred to as a "patient illness" model. To ruffle the feathers of the physician could lead him to take "his" patients to a rival institution (Ummel, 1997). Consequently, physician and hospital interests were often in opposition to one another. Physicians had little incentive to work for the corporate benefit of the HCO.

Purchasers of care, both public and private, are no longer willing to accept the high cost of medical care the old system produced. It is estimated that one out of every seven dollars in the US is spent on health care. In 1993 alone, over \$900 billion was spent on health care in the United States (Keever 1997). Purchasers of health care and the patients they represent have demanded a move from a "patient illness" model to a "resident or member wellness" model involving capitation. In the patient illness model there is little financial incentive for the physician or the hospital to concentrate efforts on keeping the patient well. The physician and the hospital receive payment only when the patient becomes ill and seeks care. Under capitation, the organization responsible for care is paid a set fee per member per month (PMPM). The incentive for the responsible organization is to keep the member well because if the member is ill resources are expended to deliver care. Although providers of care negotiate the PMPM fee with the purchasers of care, the provider organization now has a huge incentive to keep the member out of the hospital. The cost of care has shifted to the organization providing care. This risk shift causes health care provider organizations to need better information

about the health risk attributes of their patients if they are to set economically viable prices for the services they furnish and enlist the aid of physicians. (Dowling, 1997).

In order to gain control of their costs, provide a comprehensive list of services for enrollees, and market their services, many health care institutions are developing a "continuum of care." A "continuum of care" (COC) is "a customer-oriented, seamless system composed of both services and integration mechanisms that guide and track patients over time through a comprehensive array of health, mental health and social services, spanning all levels and sites of care, improving over time the health status of a defined population." (Ummel, 1997) A typical patient flow scenario of the continuum of care appears in Figure 1.

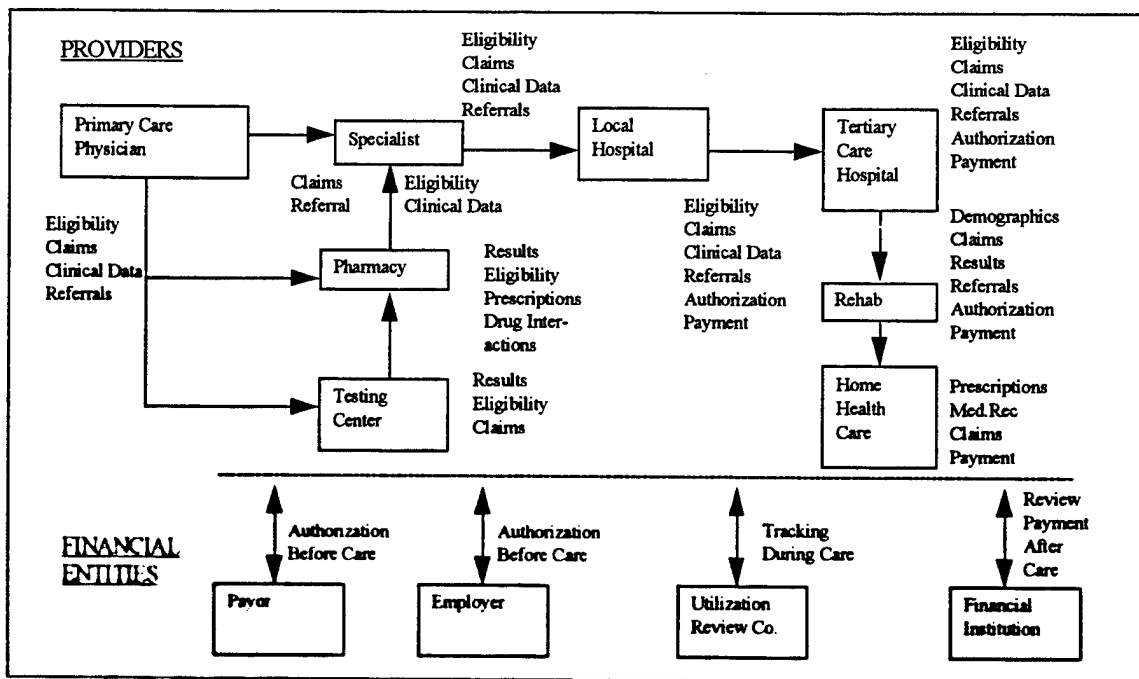


Figure 1 Patient Flow Scenario in the Continuum of Care. (After Kever, 1997)

The COC concept has vast implication for the medical CIO. Applications must evolve to support the interdisciplinary and multi-institutional needs of this new environment as the provider organization vertically integrates and introduces new, or revises old service lines. IT and applications must be flexible, interactive and support multiple goals. A logical technical architecture will develop that redefines the traditional boundaries of applications and establishes clinical practices as the center of both production and information for the COC organization.

The integrated delivery network (IDN) is an effort to meet the needs of the COC. The IDN has seven marketing aims for the HCO. They are to leverage selling by marketing the COC, form the COC, reengineer services to meet the COC, improve quality, reduce costs, accept risk and cover an entire market. The medical CIO must focus his attention on the business and in the case of a capitated managed care environment that business is ensuring the wellness of all of the "covered lives" the organization serves. Information systems must be able to integrate such diverse areas as billing, collection, case management, medical record, registration, referral, clinical management, financial policies, culture, and human resource policies. (Ummel, 1997) This requires the sharing of information ranging from individual patient data through entitlement and enterprise production information in real time (Dowling, 1997). Knowledge and information management are absolutely essential in the IDN environment.

The cancer center at the Healthsystem Minnesota presents a typical case to illustrate the COC and IDN environments and the civilian medical CIOs role.

Healthsystem Minnesota is the result of a 1993 merger between Methodist Hospital and a 450 doctor clinic. Its goal is to become an integrated delivery network by focusing on patient care as its core activity. The cancer center is the focal point of the Healthsystem's first formal clinical integration effort. The objectives of this first effort are to document the current patient care process, identify the ideal patient care process, then determine how to use IT to enable the ideal process. (Appleby, 1997)

The cancer center represents a microcosm of the range of care in the hospital environment encompassing inpatient, outpatient and home care areas. The entire cancer center program includes a special care floor in the hospital with 150 staff members, a home health agency, two outpatient intravenous chemotherapy sites, a six doctor outpatient clinic, another solo medical practice, plus bone marrow transplant, pastoral care and music therapy programs. Currently the system has 47 computer systems and 50 different medical records that contain patient information. To register a new patient, seven doctors and staff members ask for the same information. The project has determined that the answer to this problem is to develop business rules for the idealized system and design an integrated IT architecture that will support a clinical data repository with customized displays of patient information over a private intranet. The Healthsystem Minnesota CIO was a key player in helping to identify the current work process using software similar to animated engineering drawing software and in using IT to enable the clinical processes. (Appleby, 1997)

Though heavy users of technology, the health care use of IT is 10-15 years behind such industries as banking, the airlines and manufacturing (Raghupathi, 1997). The health care industry tends to lag behind other industries in IT and the development of the CIO concept for several reasons. Until recently, hospitals had an autonomous and independent culture. As mentioned earlier, there has been a separation between physician and hospitals. This isolation of physician from HCO can cause grave danger for a patient. A General Accounting Office (GAO) report on concerns voiced about electronic medical records recently showed that 30 percent of the time, when people are medically treated, information needed is not available. The GAO survey goes on to indicate that far more people are harmed by a lack of information in today's environment than will ever be harmed in an environment where medical records are available (Garets, 1997). The focus of hospital purchasing and power has been on the department, not the organization. IS departments often report to the Chief Financial Officer whose focus was on cost containment. Because of this reporting structure, there is a lack of interest in IT on the part of many Chief Executive Officers (CEOs). Until very recently, many of the vendors of medical ISs and IT were financially fragile, since it is a niche market. Because of the high cost of medical technology, the focus of technology spending is often on the clinical tools at the expense of infrastructure. Even so, industry experts say the health care industry spent \$16 billion on IT in 1996 (Raghupathi, 1997).

The new focus on the COC and the IDN and the need to control costs while improving quality due to pressures from managed care operations is changing the

information needs of the health care industry and elevating the CIO concept to the strategic level. With the demand for information by myriad members of the health care team and the recognition that knowledge and information are strategic assets in the HCO, the CIO in a civilian medical environment has become the enabler of the health care delivery process. The need to support expert systems such as clinical pathways and protocol systems, executive information systems and an information architecture are now a cost of doing business in a HCO (Ummel, 1997).

*b. Extra-Organizational Forces*

It becomes difficult to separate the internal from the external environment when discussing IDNs. The line is seldom drawn in indelible ink and can move according to the marketing needs of the organization. Every care provider owns portions of the IDN and buys services that it does not directly own. This can run the gamut from organizations like Kaiser-Permanente that own virtually an entire IDN to organizations that act as "general contractors" and own none of the organization. There are extra-organizational forces that affect the civilian medical CIO. These include the expansion of managed care, the interest of IT enterprises, government involvement, and public and health services demands.

Purchasers of care have demanded structured and affordable care packages for those they represent. Managed care health plans are meeting this demand. In 1991, managed care providers accounted for 57% of the health care market. Just three years later in 1994, managed care providers owned 71% of the market (Kongstvedt, 1996).

Managed care organizations now intervene in clinical decisions so frequently that it is difficult to find a health plan that does not require precertification for inpatient care or outpatient surgery. Most have some form of utilization review. Individual HCOs increasingly have formed alliances with forms of managed care in an effort to remain economically viable. Both parties realize that increased information sharing is mutually beneficial. (Dowling, 1997)

Information technology enterprises now realize that the technology infrastructures they developed for other industries are applicable to the information intensive health care industry. Several major vendors of ISs have taken an interest in the health care industry and entrepreneurial niche organizations are now finding health care a lucrative market. As a result, many IT corporations have an interest in health care and the health care market has become part of their corporate marketing strategy. (Dowling, 1997)

There are three separate roles the government plays in health care:

- the provider of care role;
- the buyer of care role;
- the regulator and legislature role.

The DOD medical services, the Department of Veterans' Affairs and Indian Health Services all provide patient care and are being forced to operate like private sector HCOs. The DOD medical services specifically begin capitation financing in fiscal year 1998 and will be in competition with the rest of the market place for what formerly were patients



who were required to use their services. As a buyer of health care, government interests mirror those of large corporate purchasers of health care. Government buyers of health care are moving toward managed care options for their patient populations. In their provider and buyer role, the government's information needs resemble those of the private sector areas. (Dowling, 1997)

In their unique regulator and legislator roles the government information needs involve the areas of basic medical research, epidemiological surveillance, health care research, quality assurance, and other diverse functions. These activities require information of a nature, consistency, quality and specificity that are distinct. The information needs of these activities are going to increase. Agencies such as the Department of Health & Human Services, the Food and Drug Administration, and the Center for Disease Control have been engaged in creating a health information network for years. They and other government agencies have encouraged the development of information and technology standards, creating standard medical and care delivery code structures, and national minimum data sets. Several government agencies are helping develop legislation in Congress dealing with confidentiality, privacy, and security. (Dowling, 1997)

ISs and IT are concerns of a whole host of community entities with interest in health care. Numerous institutions and think-tanks conduct clinical, health policy, clinical outcomes, and health informatics research and all are looking for data. Health care performance evaluation organizations like the National Committee on Quality Assurance

and the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) act in quasi-societal or quasi-governmental capacities and have interest in collecting and sharing data. Part of JCAHO's mission is to be a national provider of health and quality information and for their triennial health care delivery audits to become a part of all HCO's continual process improvement. The growth of the internet and proliferation of health related web sites are another method for consumers to obtain health care related information. (Dowling, 1997) All of these organizations and forces are driving the formation of health information networks and as such are factors in the civilian medical CIOs world.

### **3. Professional Organizations and Credentialing**

Medical CIOs can become affiliated with a number of organizations. The author will discuss the two most widely recognized professional organizations. They are the Society for Information Management (SIM) and the College of Healthcare Information Management Executives (CHIME).

SIM is a group of over 2700 IT executives who are corporate and division heads of IT organizations, their management staff, leading academicians, consultants and others. SIM's mission is to "provide international leadership and education in the successful management and use of IT to achieve business objectives." (SIM, 1997) It does this through active local chapters all over the U.S. and in Italy and Korea and through its own on-line discussion groups and database resources available on their web site. Meetings of

the local chapters feature speakers and discussion groups. SIM does not have a credentialing mechanism. (SIM, 1997)

CHIME is the major professional organization for medical CIOs. It was formed in 1992 as an off shoot of the Health Information Management Systems Society. CHIME's mission is to serve the professional development needs of health care CIOs and to advocate the more effective use of information management within health care to improve health care delivery. From an initial membership of 250 members in 1992 CHIME has grown to a membership of 600. It offers spring and fall CIO forums, a one week Information Management Executive course twice each year, a yearly emerging technology course, a searchable database available on its web site and a fax back document service for reference documents. CHIME does not have any formal credentialing mechanism. (CHIME, 1997)

## **B. OVERVIEW OF CHIEF INFORMATION OFFICER IN A DEPARTMENT OF DEFENSE SETTING**

### **1. Introduction**

Several factors brought about the IT and acquisition reforms of 1996. The federal government spends a huge amount of money on ISs and IT. In 1997 the federal government budgeted \$26.6 billion on IT plus another \$25 billion on unreported DOD software (Corbin, 1997). The general public perceives the government as technologically backward when compared to the private sector. While the public can cite examples of companies such as Wal-Mart and Federal Express that use IT to cater to its customer's

needs, the public finds it difficult to see similar examples in the federal government (Laurent, 1997b). Finally a series of expensive, late and unsuccessful IT programs infuriated the public in general and the Congress in particular. The four debacles most often cited are:

- The Federal Aviation Administration's (FAA) \$37 billion modernization of air traffic control that was completely restructured in 1995 after its cost had tripled. The current system is so old the FAA is buying vintage vacuum tubes from Poland (Deagon, 1996).
- The Internal Revenue Service's Tax Modernization System that is likely to exceed \$8 billion with no gains in efficiency or revenues collected. The current system has an over \$70 billion backlog in uncollected taxes (Deagon, 1996).
- The General Accounting Office's (GAO) report that said the DOD's seven year corporate information management initiative spends \$3 billion a year to modernize automated systems without significant benefit.
- The National Weather Service's \$5 billion modernization that is currently five years behind its initial completion date. (Laurent, 1997b)

Congress passed and on February 10, 1996, President Clinton signed the National Defense Authorization Act for fiscal year 1997. It contained two provisions that combined with the Federal Acquisitions Streamlining Act of 1993 dramatically changed the focus of federal IT from a technical issue to a management issue. The two provisions are Division D, the Federal Acquisitions Reform Act (FARA) and Division E, the

Information Technology Management Reform Act (ITMRA), also known as the Clinger-Cohen Act. ITMRA's author was the then Senator from Maine and now Secretary Of Defense William R. Cohen.

The increase in public scrutiny, tighter budgets and legislative mandates all compel IT managers to focus their attention on managing IT investments, rather than focusing too narrowly on IT acquisitions. ITMRA repealed the 30 year old Brooks Act that previously gave exclusive authority for federal IT procurements to the General Services Administration (GSA). Now each agency has authority over its IT programs while OMB has general oversight over all federal IT programs, as the executive agency in charge of overseeing all federal budgets (Khoury, 1997). President Clinton's July 17, 1996 Executive Order 13011 operationalized these laws into policy for the DOD (Clinton, 1996). Together this legislation and Executive Order provide a government framework for capital planning and performance based management to improve how each agency acquires and manages IT.

## **2. ITMRA Mandate**

### ***a. Background***

Formerly the focus of IT procurements was on technical details such as the capabilities of the hardware and software, the new focus after these legislative initiatives is on business performance related issues. The legislative reforms treat IT as an investment to be measured in terms of cost savings via return on investment (ROI), faster service

delivery, efficiency improvements, increased customer satisfaction, and even consider whether the procedure of applying IT to a process should be performed at all (Laurent, 1996b). Agency heads are responsible for ensuring that their agencies effectively use IT to improve mission performance and service to the public (Clinton, 1996). Areas of interest to be further discussed include creation of the CIO and the CIO council, Capital Planning, Performance Measures, Purchasing, Competition, Modular Contracting, the Information Technology Resources Board, and the Government Information Technology Services Board. These areas define the responsibilities and corresponding core competencies needed for a DOD CIO to be effective.

*b. Chief Information Officer and Chief Information Officer Council*

ITMRA mandates that agency heads appoint a CIO, who reports directly to the agency head. The CIO is to have information resource management (IRM) as his official primary duty, "monitor the performance of IT programs for the agency, evaluate the performance of those programs on the basis of applicable performance measures and advise the head of the agency regarding whether to continue, modify or terminate a program or project." (ITMRA, 1996) The CIO must promulgate and sell a strategic plan which establishes performance goals in objective, quantifiable and measurable form, establishes performance indicators to be used in measuring relevant outputs, provides a basis for comparing actual results with performance goals, and describes the means to verify and validate measured goals.

Other responsibilities include providing advice and assistance to the agency head and other senior managers on the acquisition of IT and management of information resources and developing and maintaining an integrated IT architecture for the agency. Under Clinger-Cohen, the CIO must assess requirements established for agency personnel regarding their knowledge and skill in IRM and in facilitating the achievement of performance goals established for IRM. He then must assess how the positions and personnel at the executive and management levels of the organization are meeting those requirements and develop plans for hiring, training and professional development of personnel. (ITMRA, 1996)

The CIO council is the principal interagency forum to improve agency practices. The CIOs and deputy CIOs from 28 executive agencies plus two representatives from selected other agencies comprise the CIO council. The Deputy Director for Management of OMB chairs the CIO council. The Vice Chair is an agency CIO elected by the CIO council on a rotating basis. This group will make overall IT management policy, procedures and standards for federal government agencies, share best practices, sponsor cooperation in using information resources, and set hiring and profession development standards for information management for the executive agencies. They also are to make recommendations to executive agencies and organizations on the government wide information resource management strategic plan required by the Paperwork Reduction Act of 1995. (Clinton, 1996)

*c. Capital Planning and Performance Based Management*

Just as a private business would not invest in property or portfolios unless the business predicted a positive return on investment, now federal agencies under ITMRA must apply this same philosophy to IT acquisitions. Agencies must manage their IT programs as if each were a capital investment, keeping in mind that mission benefit, not cost or schedule, must be the overriding measure of success for an IT project. It is how IT contributes to mission accomplishment that is the deciding factor for investment purposes (Paige, 1997b). The decision to begin an IT project should involve the same kind of investment considerations that might go into a decision to purchase stocks, real estate, or build a new building.

The first step in the decision process is to answer the following three questions before the agency applies IT to a process:

- Should the government perform the function?
- If the government should perform the function should it be kept in house, moved to another agency or to the private sector?
- Is the function being performed in the most efficient manner or should it be reengineered? (Corbin, 1997)

After the above determinations are made, agencies must develop a capital investment plan for IT. They must perform cost/benefit analyses, report the expected ROI, do risk analyses, identify benefits and impacts on other agencies, and develop performance measures before investing in IT (Laurent, 1996a).



Clinger-Cohen makes specific reference to using performance measures and performance and results based management. According to ITMRA, executive agencies must use performance measurements. The performance measurements must measure how well IT supports the programs of the agency. The DOD defines IT performance measurement as "the assessment of effectiveness and efficiency of IT in support of the achievement of an organization's mission, goals, and quantitative objectives through the application of outcome-based measurable and quantifiable criteria, compared against an established baseline, to activities, operations, and processes." (Paige, 1997b) Performance measurement requires that executive agencies benchmark their agency performance measures against comparable processes and organizations in the public and private sector for such things as cost, speed, productivity and quality of outputs and outcomes. Successful performance measurements produce measures that are significant, linked to outcomes, correspond to a baseline, and are based on credible information (Paige, 1997b).

The DOD suggests a six step generic method for measuring the IM/IT performance of an organization, program, or project. They are to:

- define the mission, key result areas and business functions;
- develop mission related goals;
- generate performance measures;
- validate and verify performance measures;
- implement the performance measures and collect data;

- monitor and assess the results and repeat the process as needed. (Paige, 1997b)

Each step in this six step method has several questions associated with it. They are available in Appendix A.

OMB has authority for several aspects of federal IT acquisitions. OMB oversees federal IT procurement just as a fund manager oversees a portfolio of investments. OMB analyses, tracks and evaluates “the risks and results of all major capital investments made by an executive agency for information systems” (ITMRA, 1996). This is done by analyzing, for the life cycle of each system, the projected and actual cost, benefits and risks, and reporting this analysis to Congress in the President’s budget each fiscal year. Agencies must analyze risk prior to entering into IT contracts by doing risk identification, risk assessment and risk management. OMB will develop methods for measuring the success of specific IT procurements by focusing on performance and results.

To help federal agencies achieve their goals, the GAO studied successful private and public sector organizations to learn the which factor influence success in results based management of IT investments. OMB has developed a Capital Programming IT Investment Guide with eight concepts of capital investment management. To receive OMB approval for funding an agency must demonstrate that an IT investment:

- supports core government functions;
- is being considered because no alternative source can support the function;

- supports work processes that have been simplified to reduce costs and improve effectiveness;
- demonstrates a ROI that is equal to or better than alternatives;
- is consistent with federal, agency and bureau information architectures;
- reduces risk by avoiding custom designed components, using fully tested pilots and securing substantial user involvement;
- will be implemented in phases;
- employs an acquisition strategy that appropriately allocates risk; between the government and the contractors. (Khoury, 1997)

*d. Modular Contracting and Purchasing*

Clinger-Cohen requires that a modular contracting approach be used for purchasing major systems. ITMRA says that “under modular contracting, an executive agency’s need for a system is satisfied in successive acquisitions of interoperable increments.” (ITMRA, 1996) By using common or commercially accepted standards applicable to IT each increment will be compatible with other increments of the system. The purpose of modular contracting is to avoid the huge contracts that produced systems that were often generations behind the state of the art by the time they were delivered. Using standards and buying small modules over time helps incorporate the state of the art technological advances into the system. Also modular contracting makes contract

management easier by breaking the complex challenges inherent in a large contract into small segments which are more efficiently managed (Khoury, 1997).

One of the main goals of this new legislation is to introduce a sense of timeliness into the purchasing of IT. With the repeal of the Brooks Act, agencies are now free to buy what they want as long as they comply with government wide standards. ITMRA significantly reduced the opportunities for bid protests that have often tied up contract awards for months and even years (Bauer, 1996). The primary methods of acquiring IT resources are not subject to protest. GAO will hear IT protests but imposed new deadlines on the protests. GAO must make a decision on a protest within 100 calendar days after the filing of the protest. Under Clinger-Cohen, agencies must award IT contracts within six months of solicitation release or the competition should be canceled. Product delivery should occur within eighteen months of contract award or the agency should terminate the contract. (Khoury, 1997)

*e. Competition*

The real strength of Clinger-Cohen comes from vesting power in the hands of OMB, rather than GSA, for managing IT acquisitions. Agency heads must report annually to Congress on the effectiveness and efficiency improvements made using IT (Laurent, 1996a). Congress expects agencies to cut IT costs five percent per year and use IT to increase efficiency of operations five percent per year (Laurent, 1996b). When OMB does its annual report to Congress it will compare agency IT performance reports. Potential IT investments will be traded off against one another and balanced with non-

technical investments. OMB can recommend increases or reductions in agency budgets. It can also designate an executive agent to hire a contractor to manage the agency's IT acquisitions or information resources if OMB determines the agency is not managing its these functions wisely (Laurent, 1996a). ITMRA authorizes OMB to kill budgets for systems deemed ineffective, duplicative, and wasteful. OMB will force accountability through the budgeting process.

*f. Information Technology Resources Board*

In the fall of 1993, the GSA established the Information Technology Resources Board (ITRB) to make recommendations for improving the IT acquisition process (ITRB, 1997). With the passage of Clinger-Cohen the OMB assumed sponsorship of ITRB. Senior government IT management, technical and acquisition managers who work in small teams to review system design, development and acquisition management plans constitute the ITRB (Porter, 1996). Each team member typically devotes 25% of his work week to an ITRB project team. ITRB initiates reviews at the request of both OMB and an agency to assess the status of a system. The board makes recommendations on next steps but does not assume responsibility for a project. The board will periodically publish lessons learned and best practices based on completed reviews.

ITRB supports the Presidential Technology Team concept. The Presidential Technology Team brings together groups of IT experts from across government on a temporary basis to the ITRB. These teams will be available to assist

agencies for six to eighteen months on particularly difficult IT problems. Each participant commits themselves full-time to the project and gains valuable experience while the agencies gain needed help. The ITRB assists an agency in the selection of candidates for the Presidential Technology Team (ITRB, 1997).

*g. Government Information Technology Services Board*

While ITRB concentrates on systems already under development, the focus of the Government Information Technology Services Board (GITSB) is on the future and to IS projects that cross agency boundaries. The mission and purpose of GITSB is to "ensure continued implementation of the IT recommendations of the National Performance Review and to identify and promote the development of innovative technologies, standards and practices among agencies and State and local governments and the private sector." (Clinton, 1996) Its focus is on fields such as defense, health care, environmental protection, law enforcement and electronic commerce where cross-agency cooperation can eliminate duplication and waste and provide a common, shared infrastructure for IT. Agency experts promote cross-agency cooperation and intergovernmental approaches to support common operational areas, develop and provide government wide shared infrastructure services for multiagency projects, and create interagency "affinity group" focuses on business areas for related business or technology areas (Clinton, 1996). GITSB along with the GSA Interagency Management Council have awarded millions of dollars of ITRB venture capital as start-up cash to innovative projects for delivering these types of benefits and services (Porter, 1996).

### **3. Credentialing of DOD CIOs**

As stated earlier in section 2b of this chapter, the Clinger-Cohen Act of 1996 requires that federal agencies ensure personnel at the executive and management levels have the knowledge and skills required to achieve performance goals established for IRM. The CIO council's CIO Training Program Subgroup identified federal CIO competencies. A list of ten subject areas that relate directly to the federal CIO competencies and build on the these competencies, is the basis of the CIO Certification Program. The ten subject areas are Policy, Strategic Planning, Leadership/Management, Process Improvement, Capital Planning and Investment, Performance and Results-Based Management, Technology Assessment, Architectures, Security and Acquisitions. (IRMC, 1997)

Fort McNair, Washington D.C. is the home of the Information Resources Management College (IRMC). It is part of the National Defense University which focuses on professional military education. IRMC maps the subject themes of the core competency areas to the courses to teach required competencies. There are one or more primary course offerings that allow a student to acquire related competencies. The student must finish a total of eight, five-day courses or be part of the Advanced Management Program supplemented by a lesser number of courses, depending on the track and electives taken through the Advanced Management Program. Also, the student must complete two more courses selected from either the primary or enrichment listings for any subject area. All students must successfully finish the subject areas of Policy and Performance and Results-Based Management to receive their completion certificate. The

student must also complete four more subject areas through primary course offerings.  
(IRMC, 1997)

To be eligible to attend, civilian students must be grade GS/GM 13-15 and military students grade O5-O6 and possess a bachelor's degree. IRMC considers waiver requests for applicants within one grade level of the required grade. IRMC teaches all courses at the graduate level and includes student assessments to achieve academic rigor. The student assessments take various forms from individual papers and projects to team projects and presentations. Instructors teach principally in seminar format. Lectures, guest speakers, and field studies supplement the seminars. The IRMC awards a completion certificate when a student completes the required courses. The DOD CIO sponsors the program. (IRMC, 1997)



### **III. METHODOLOGY**

#### **A. DISCUSSION OF CRITICAL SUCCESS FACTORS**

##### **1. Introduction**

John Rockart developed the concept of Critical Success Factors (CSF) at the Sloan School of Management, Massachusetts Institute of Technology, in the late 1970's. Originally developed to help executives define their information needs, Rockart says that the concept is useful for more than information system design. It is useful at both the executive and management levels of the organization and for the management process in general. Critical success factors define those areas in a business environment where things must go right for the business and the person managing that business to succeed. They are the executive's essential conditions for success. Rockart's team of researchers identified four sources or areas where executives must search for critical success factors. They are:

- the structure of the particular industry;
- the company itself;
- the environment;
- temporal or time-dependent factors. (Rockart, 1979)

##### **2. The Structure of the Industry**

Each industry has its own particular critical success factors determined by the characteristics of the industry. For instance, it may be essential in the automotive industry

to have a quality dealer system, however this factor means nothing in the health care or grocery industry. Likewise, in a government health care system it may be essential to have all hospital pharmacy drug formularies contain the same medications, but this factor has nothing to do with the automobile industry or the civilian health care industry. Executives ignore these factors at their own peril. The executive must know his industry and understand what its critical success factors are. (Rockart, 1979)

### **3. The Company or Organization**

Just as each military service has its own culture, each company in an industry is its own unique situation. Its individual situation is determined by its history, industry position, geography, management team, and competitive strategy. For example, for a smaller company in an industry dominated by one or two large firms, the actions of the industry leaders can force smaller firms to seek a niche market or drop certain product lines. Every executive must understand these factors. Also for an executive to succeed in his company he must understand his company's internal politics and centers of power. (Rockart, 1979)

### **4. The Environment**

As the stock market rises or falls and the economy reacts, as political parties gain or lose power, and as the ethnic environment of a market changes, critical success factors can change. The environment identifies sources of critical success factors that are subject to change regardless of the changes involved in the industry or the company. Rockart

used the example of the energy crisis of the mid-1970s. Prior to 1973, virtually no executive in the United States would have considered the availability of fuel as a critical success factor. With the establishment of the oil embargo by certain oil producing nations, the cost of fossil fuels skyrocketed. The successful executive must monitor the external environment for critical success factors. (Rockart, 1979)

## **5. Temporal Factors**

Some internal organizational considerations lead to temporal critical success factors. They are factors that become critical because they are below the threshold of acceptability at a particular moment in time. For example, if an entire executive team dies in a plane crash, the objective of rebuilding the executive team would then become a critical success factor. One source of temporal factors for CIOs is surveys of CIOs and their CEOs in industry trade journals that ask each group to define the top CIO management and information technology issues. The results of the surveys provide a prioritized list of temporal factors. This critical success factor speaks to an executive's ability to manage in a changing environment. (Rockart, 1979)

## **B. DISCUSSION OF SURVEY METHODOLOGY**

At the Navy medical CIO Conference/CHIME "Information Management Executive Course," Cleveland, Ohio, June 1997, the author conducted a survey of Navy medical CIOs. The two week course was held at Case Western Reserve University, and conducted through the Health Systems Management Center of the Weatherhead School of

Management and the College of Healthcare Information Management Executives (CHIME). The Naval Medical Information Management Center (NMIMC), Bethesda, Maryland, funded the course. NMIMC was established in 1961 to improve, develop and distribute new information technologies in support of Navy Medicine's commitment to patient care. Its mission is to "plan, coordinate, and provide comprehensive, integrated, cost-effective information management capacity throughout the world in support of health services across the continuum of peacetime and military operations." (NMIMC, 1997) The Commanding Officer of NMIMC functions as the CIO for the DON Bureau of Medicine and Surgery.

The faculty members for the course are nationally recognized leaders in health care. The Health Systems Management Center of the Weatherhead School of Management developed a series of health care executive education seminars for professionals, executives, and managers from all sectors of the health care system. The seminars were presented during the first week of the course. CHIME's "Information Management Executive Course" course was presented during the second week of the course.

Due to funding, a limited number of seats were available for the conference. The participants at the conference were nominated to attend and represent seventy percent of DON medical personnel who are their command's senior military person in the IS department. As such they represent the Navy medical equivalent of a CIO.

The survey was designed to determine Navy medical CIO's opinions of what core competencies a Navy CIO requires. Each respondent was asked to provide demographic information and respond to a series of questions to determine if they are a CIO, using a definition to be described in a later section of this thesis. The author developed a list of fifty-three potential core competencies from numerous sources (Bergman, 1994) (Burbridge, 1994) (Frenzel, 1992) (Frew, 1996) (CHIME, 1997) (Gartner, 1996) (IRMC, 1997) (ITMRA, 1996) (Paige, 1997a) (SIM, 1997) (Sprague, 1993). Respondents were asked to circle "yes" or "no" next to each potential competency to provide their opinion of which competencies constitute core competencies for a Navy medical CIO. The author also conducted interviews and discussions with the participants of the seminar to determine their view on current and potential measures of effectiveness for Navy medical CIOs. The title and job responsibilities many of these personnel hold are the subject of this thesis and their opinions represent CIOs in the field, a valuable data point. A copy of the survey appears in Appendix B.

### **C. DISCUSSION OF THESIS METHODOLOGY**

The purpose of this thesis is to determine the core competencies and measures of effectiveness for Navy medical CIOs. The author begins by defining a set of responsibilities of a civilian medical CIO and a DOD CIO. To define the responsibilities of a civilian medical CIO and a DOD CIO, the author uses a critical success factor model. Using the background section of this thesis to identify various factors about each type of CIO's industry, organization, environment, and time related issues, the author develops a

list of critical success factors for both a civilian medical CIO and a DOD CIO. The author reviews each critical success factor and selects applicable core competencies from the list of potential core competencies developed for the Navy medical CIO survey. Core competencies are proficiencies that a CIO must have if he is to be successful at a critical success factor. A core competency can be contrasted with a skill. A true core competency is essential to be successful while a skill is something that is nice to have. Without a skill, a person can still succeed as a CIO in meeting the critical success factor. The author again analyzes each critical success factor using the list of core competencies applicable to the critical success factor, to determine if there are any other factors needed to successfully meet each critical success factor. The author then enumerates a list of core competencies for a civilian medical CIO and a DOD CIO.

By combining these two groups of core competencies and skills, this thesis develops a set of core competencies and skills necessary for a Navy medical department CIO. A survey of Navy medical CIOs provides input into what the Navy medical CIOs in the field think are the core competencies they need to succeed in their environment. The author uses the survey results to validate his determination of a set of core competencies and skills of a Navy medical CIO. The author reviews each of the core competencies of a Navy medical and develops a set of proposed measures of effectiveness. A Navy medical CIO can use measures of effectiveness to gauge his effectiveness in contributing to the executive management of the Navy hospital.

## **IV. FINDINGS**

### **A. RESPONSIBILITIES OF CIVILIAN MEDICAL CHIEF INFORMATION OFFICER**

#### **1. Introduction**

According to Rockart, critical success factors are related to the structure of the industry of the executive, the organization in which the executive works, the environment, and temporal factors (Rockart, 1979). For the civilian medical CIO, the industry is health care and the organization is a health care organization. As discussed in Chapter II of this thesis, the health care industry is information intensive. There is a need to share information inside and outside the HCO to support the continuum of care concept, integrated delivery network and the computerized patient record. The environment is the managed care concept of member wellness that focuses attention on keeping the patient healthy. A temporal factor involves the fact that health care lags behind other information intensive industries in development of the CIO concept. Current surveys of CIO and CEO concerns will determine other temporal factors (Gartner, 1996) (Rowe, 1997) (SIM, 1997). The critical success factors for a civilian medical CIO as defined by the author of this thesis are to:

- align the IS function and activities with the organization's strategies;
- strengthen the role of CIO in the organization;
- create, alter and manage the composition and characteristics of the IT asset;

- make clinical information systems more useful and relevant to clinicians;
- facilitate the transition to the Integrated Delivery Network;
- develop methods to handle security, privacy and confidentiality concerns.

## **2. Aligning the Information Systems Function and Activities with the Organization's Strategies**

In the eighth annual CIO Magazine/Ernst & Young survey of CIOs and their CEOs concerning the CIO's role and function in an organization, both groups agreed that aligning IT and corporate goals is the CIO's most important function and will add the greatest value to the future of the business (Row, 1997). Successful organizations must treat IT as an enabler to its strategic and business plans, not a separate strategic direction. Research indicates that organization's that succeed with their IS programs do not discuss and assess them separately from other investments (Earl, 1993). Some health care industry CIOs even suggest that there be no separate IT strategic plan. Strategic plans have no beginning or end. IT strategy should be a regular management discussion. They further state that ISs have no value apart from the organizations' strategies and plans but must come from, support and be imbedded in these strategies and plans. (Glaser, 1997a)

To properly align the IS function with an organization's strategies requires buy-in from and shared decision making among the CEO, top executives, and the rest of the organization. Alignment is not about vision statements or goals that the IS and non-IS executives are attempting to attain. Alignment is about process, and what management does to achieve its goals (Luftman, 1997). The CEO's support of the value of ISs is the



starting point for the alignment process. A CEO who believes IT is critical to the success of the business is likely to see the value of having the IS function aligned with the business function. CIOs must deliver some benefit or value to the CEO and the business in order to forge good CEO/CIO relationships. Alignment also requires support from other top executives in the organization and involves shared decision making among the IS manager and those managers in the rest of the organization. ISs are often only one of several investments needed for an initiative to succeed. The top management group must believe that all investments in a venture are identified, well defined and their inter-relationships understood (Glaser, 1997b). This requires the concurrence of the entire management group and then buy-in from the rest of the organization. The concepts of CIO, CEO and executive management relationships are further discussed in the section entitled "Strengthening the Role of Chief Information Officer" that follows.

One model for strategic alignment is the Component Alignment Model (CAM) that has evolved from Henderson and Venkatraman's Strategic Alignment Model and is particularly applicable to the health care environment. According to the CAM, it is not sufficient to harmonize business strategy with IT applications. It is necessary to align IT infrastructure, processes and people, the organization's infrastructure, processes and people, business strategy and IT strategy. Using the CAM, IT evolves from a support role to a strategic role that redefines the business scope. (Martin, 1997)

Using the CAM requires three steps. Step one is the continuous assessment of seven components divided into uncontrollable and controllable components.

Uncontrollable components include the external environment and emerging information technologies. Although they are uncontrollable they must be understood. Controllable components are the organization's mission, organizational infrastructure, processes and people, IT infrastructure, processes and people, business strategy, and IT strategy. Step two involves the alignment of controllable components in response to non-controllable components. Step three is the alignment of controllable components among themselves. (Martin, 1997) A graphic representation of the CAM appears as Figure 2.

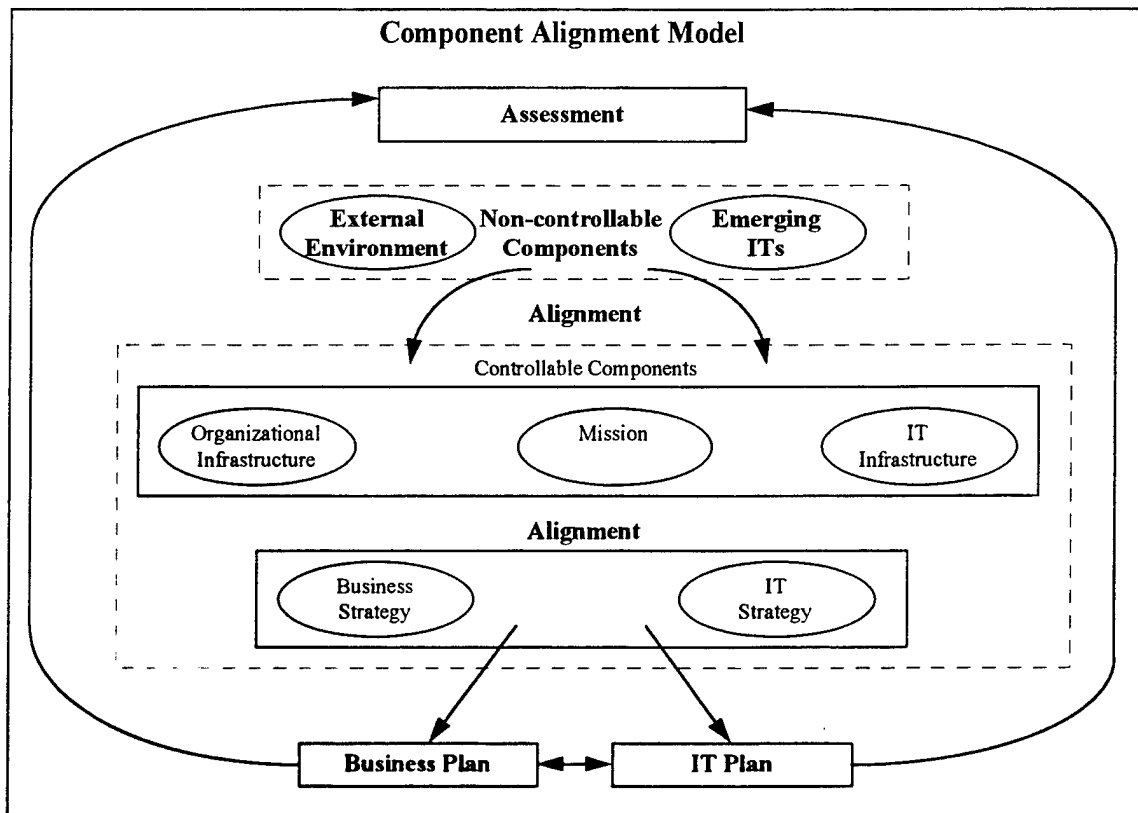


Figure 2. Component Alignment Model. (From Martin, 1997)

ISs do not exist in a vacuum and have no value in themselves. They are enablers. They are also no different from any other asset of the organization. Financing of IT as

well as financing for the Laboratory, Pharmacy, Patient Administration or any other department in the hospital is best done at the institutional level. Priorities for ISs and other departments are best determined at the executive level and for the benefit of the entire organization.

### **3. Strengthening the Role of Chief Information Officer**

Strengthening the role of CIO within an organization is closely related to aligning the IS function and activities with an organization's strategies. Information technology and the CIO are integrators of the continuum of care. As the decentralization of IT and the growth of end-user computing continue, IT increases in strategic importance for health care organizations and as such requires input and direction from the CEO and the organization's top management. The key to strengthening the role of the CIO is developing an excellent working relationship with the CEO and the organization's senior management team. Good executive relationships can save you when things go wrong and poor ones will sink you "faster than the Hindenburg in flames." (Pastore, 1996)

In most organizations the CEO establishes the enterprise wide direction for the organization including the organization's acceptance and use of technology. The CEO can agree that IT is an enabler in solving business problems or that IT is an expense to be tightly controlled. The CEO molds the corporate culture. Corporate culture must support the innovative application of IT in order for the CIO to work effectively. A successful CIO must be able to communicate the added value of IT investments. Communicating directly, one-on-one, with the CEO best accomplishes this. A direct reporting relationship

with the CEO establishes the ability and personal understanding needed to enable the CIO to have needed access and trust of the CEO. Having the ear, as well as the mind and heart of the CEO, is invaluable for the CIO.

For many CEOs the primary requisite of a CIO is integrity. Although considered an essential quality for every executive to possess, integrity in a CIO is particularly important for many CEOs. Some CEOs feel especially uneasy discussing IT because of their lack of direct personal experience with technology. Others are apprehensive about IT because they are aware how difficult it is to assess IT project status, technology risk, and functional performance. How well a CIO manages IT often can make or break a CEO's success in an organization. Behavior reveals integrity. The CEO's major concerns are openness and business loyalty. The CEO needs to feel that CIO's first loyalty is to the business as a whole, not to establishing a personal empire or to having the latest and greatest technology. The CEO must be able to expect that the CIO's IT initiatives will be driven by business imperatives and not the other way around. (Earl, 1994)

In addition to developing a relationship with the CEO, the CIO must be accepted as a member of the executive team. To be accepted as a member of the hospital executive team the CIO must know the business and be able to speak the language of the business. He must be able to take the technical issues of IT and translate them into clinical and business issues. When a person travels to a foreign country, it is unreasonable to assume that every one in that country will understand the traveler's language. If the traveler wants to have a safe, enjoyable and fulfilling journey the traveler must learn the language

of the country he is visiting. It is not incumbent on the executive team to learn the IT language. The CIO must learn the jargon and acronyms of the business and speak intelligently on business issues to be accepted by other members of the executive team.

To be accepted as a member of the executive team requires that the CIO add value to the team. The CIO must have a seat at the executive table. Research has consistently indicated, that membership on the executive board, rather than reporting structure, is the critical indicator of a successful CIO (Earl, 1994). Participation at executive meetings gives the CIO enhanced access to fellow executives, increases the number and quality of relationship-building opportunities, and provides the CIO a new level of understanding of the business (Earl, 1994). More than having a seat at the table, the CIO must be an active member of the executive team. The CIO does this by building substantive executive relationships with peers based on his ability to educate and communicate the world of IT to other team members and by exhibiting the same qualities of integrity discussed earlier in the context of CEO/CIO relations.

Strengthening the role of CIO within an organization will allow the CIO to become more active in the management of the organization. It will also give the CIO the needed business focus to allow him to more strategically manage the IS function. In an industry like health care, where information is at the core of the patient centered focus and the CIO concept has lagged behind other information intensive industries, it is imperative that the role of the CIO within the organization be intensified. If the CIO does not have

the power base to optimize IT for the organization, it is doubtful that other members of the executive team will perform that function.

#### **4. Creation, Alteration and Management of the Composition and Characteristics of the Information Technology Asset**

The CIO is the custodian of the information technology asset of the organization. As such he is the caretaker and manager of an expensive and strategically important piece of the organization. Management of any asset requires the manager to understand the composition of the asset, determine the characteristics of the asset, identify how the asset contributes to the goals of the organization and be able to assess the performance of the asset. The IT asset contains several components including application systems, an IT platform or architecture, data, IS staff, and policy, procedures and organizational structures. An ideal application system improves existing operations, provides superior support to critical processes, behaves with integrity and reflects a reasoned balance of institutional priorities. The perfect IT platform is agile (easily removed or replaced), is potent and is capable of integrating applications, data, and components of base technology. High quality data is accurate, timely, complete, precise, understood and accessible. The ideal IS staff executes well, stays current in their expertise, and provides world class support and consultation services. Perfect policies, procedures and organization structures balance control and autonomy, are efficient, provide sustained political support and organizational input and enable responsiveness. (Glaser, 1997b)

The IT asset is strategically important for health care because it can advance strategies in several ways. It can reduce expenses and improve productivity at the same time. It can improve decision making by reducing errors and shrinking decision making time. As an enabler of complexity, the IT asset can strengthen or transform inter-organizational relationships. This is extremely important in the COC and IDN environment described earlier. The IT asset can monitor critical activity in the organization, enable customization and differentiation, and improve organizational coordination. (Glaser, 1997b)

The CIO has three fundamental tasks that concern creating, altering and managing the IT asset. The CIO must develop, sustain and advance a robust information technology asset. The CIO is responsible for ensuring a linkage between organizational initiatives and goals and the information system activities. Also the CIO must ensure the organization has a well managed IS function. (Glaser, 1997b)

The CIO must create, alter and manage IT asset, but occasionally this particular CSF is assumed or forgotten. A statement made by one CEO and echoed by many others is "alignment does not matter if the basics are not delivered." (Row, 1997) CEOs and the rest of the executive team expect that the day to day operations of their systems will run smoothly. They expect to be able to get on the network whenever they need to and to read e-mail whenever they want. They expect the CIO is keeping up on new technology and providing accurate technology forecasts. They expect all the attributes mentioned in the first paragraph of this section concerning ideal application systems, IT platform or

architecture, data, IS staff, and policy, procedures and organizational structures are attributes of their IT asset possesses. They also expect that the IS department will look on the rest of the organization as its customers and treat them accordingly. It is essential that the CIO and the IS staff be user driven to meet these expectations.

#### **5. Making Clinical Information Systems More Useful and Relevant to Clinicians**

Health care organizations developed and implemented their first computer based information systems almost thirty years ago (Anderson, 1997). One of the most difficult problems of implementing information systems in the health care environment has been the reluctance of many clinicians to use computers. Information systems department planners, computer science professionals and other personnel continually marvel at what, at times, seems absolute obstinance on the part of some clinicians who avoid any contact with computers. It is essential for the continuum of care concept that supports the integrated delivery network that clinicians be familiar with and use information systems. Information systems departments deliberate long and with great difficulty looking for ways to persuade clinicians to use computers.

This is the wrong approach. The question should not be; How does one persuade clinicians to use computer? The question should be; How does one make computers useful to clinicians? Clinicians, like any other group of professionals, are more likely to use information systems if the systems increase their clinical efficiency, while improving



patient care and the bottom line (Bergman, 1994). Information systems that do not meet the above criteria will fail.

Information systems have failed in the clinical environment for three reasons:

- failure of designers to recognize constraints in the clinical environment;
- failure to obtain clinician, particularly physician, participation in development and buy-in;
- failure to recognize social and organizational changes to the work place caused by introducing information systems (Anderson, 1997).

Computer science professionals and engineers did much of the early work on designing clinical workstations and clinician interfaces without input from health care professionals. This early work failed to recognize that health care professionals have constraints in their working environment. For example, physicians and nurses use both hands when examining and caring for patients so input at the patient's bedside utilizing a keyboard is impractical. Busy clinicians will discard information systems when the use of equipment and clinical ISs become cumbersome and impede the clinical process. Information systems with no sponsorship from the medical staff are also likely to fail. The introductions of clinical ISs alter traditional work flow patterns and interfere with the way clinicians organize their thought processes in caring for patients. (Anderson, 1997)

Making ISs more user friendly for clinicians involves broad clinician involvement in the selection and implementation of the ISs from the initial stages of development, considering in advance how the system will affect routine practice patterns, and designing

interfaces that are intuitive and customized for the user. Expert and artificial intelligence systems can adapt to each clinician's clinical practice patterns and to an algorithm they use in their practice. Some clinicians prefer to see laboratory results first, while others want to see vital signs first. The system should be able to anticipate the clinicians practice pattern and offer options for viewing data the way each clinician desires to see it. New technologies such as voice recognition offer promise in clinical settings. Whatever the necessary technology is, it needs to be designed to function in the clinical environment if it is going to be accepted and used by clinicians.

Under the patient illness model, with its cost based reimbursement, hospital information systems were primarily used for administrative purposes such as accounting and patient billing. With the member wellness model and the promise of the IDN, a computerized patient record (CPR) in some form is inevitable. The CPR will require that all data be entered into an information system so that it is available in archival form. Clinicians who examine the patient, order the laboratory tests, prescribe medication, and follow-up care are the natural personnel to enter much of this critical data automatically as it is generated as a by-product of the normal clinical routine. They are uniquely qualified to validate the data entered into the CPR. The CIO, who involves clinicians in developing and implementing information systems and insists that applications be useful to the clinical as well as the business sides of the house, should succeed at the critical success factor of making clinical information systems more useful and relevant to clinicians.

## **6. Facilitate the Transition to the Integrated Delivery Network**

In the health care world developed in response to capitation and managed care, the health of the patient has once again become the central focus. Information systems, therefore, need be patient-centered, not administration-centered. For civilian medical CIOs that means placing the emphasis of clinical information systems on patients health problems and needs and managing costs effectively (Bergman, 1994). The CIO must focus his attention not on the narrow scope of the hospital environment, but on the larger scope of the continuum of care concept, at health care across the community as provided by numerous practitioners in many different settings. Information systems must be able to support the COC concept and its need for integrated delivery networks and the CPR. The CPR will form the basis for a collaborative environment in which multiple clinicians and ultimately the patient will be able to engage in interactive electronic discussion (Kilman, 1997). The CIO supports these concepts by developing the infrastructure architecture for the IDN.

As discussed at length in section C3 later in this chapter, the CIO is responsible for managing the infrastructure portion of an application/infrastructure (A/I) architecture (Hoffman, 1994). Infrastructure is the underlying base technology used to develop and operate application systems. It also includes the technical and management strategies and tactics utilized to ensure the platform achieves its goals. Infrastructure decisions occur every time a new system or technology enters the environment. Forming infrastructure architecture strategies is a complex conceptual exercise requiring skill in systems analysis

and systems thinking. Defining the infrastructure may be the most important solo decision the CIO makes and is a CSF for a civilian medical CIO (Glaser, 1997b).

#### **7. Developing Methods to Handle Security, Privacy and Confidentiality Concerns.**

The hospital environment, discussed in Chapter II of this thesis with its need for a computerized patient record, requires wide dissemination of data both inside and outside the integrated delivery network. The goals of providing wide spread access to data and controlling access to data for security reasons are in direct opposition to each other (Emery, 1997). Developing policies, procedures and systems to adjudicate this incongruous situation is a temporally based critical success factor for a civilian medical CIO.

Medical records, whether computerized or on paper, contain both mundane and highly sensitive personal information. The mundane facts such as height, weight, and blood pressure are personal information, but most patients do not object to hospitals sharing this information. However topics such as fertility, abortion, emotional problems, psychiatric care, HIV status, sexually transmitted diseases, substance abuse, physical abuse, and genetic predisposition to diseases are emotionally charged hot-button issues in our society. Because of the Hippocratic Oath, the Code of Ethics of the American Medical Association, and the federal Privacy Act of 1974, patients have a strong expectation that such information will be kept private unless it is used in the context of providing care. Without this expectation, patients may avoid care, provide incomplete

data or even lie when asked for medical information. Clinicians reasonably expect accurate data to diagnose, avoid duplicative risky or expensive tests, and design effective treatment plans that consider many complicating factors. (Rindfleisch, 1997)

Health care CIOs have determined that the most significant threats to patient information can come from inside the patient care institution, within secondary user settings, or from outside intrusion into medical ISs. Inside the patient care institution, accidental disclosures, insider curiosity, and insider subordination are significant threats. Accidental disclosures occur when hospital personnel make innocent mistakes that cause unintentional disclosures. Examples include leaving information on a computer screen for unauthorized personnel to view, incorrectly addressing e-mail or fax messages, overhearing a conversation in a hospital elevator, or even a pharmacy technician filling a prescription for a friend. Insider curiosity involves medical personnel abusing their record access out of curiosity or for their own purposes. Some personnel might want to know about the disease history of a staff member they are dating or are curious about a celebrity in the hospital. Insider subordination involves a measured determined act by medical personnel releasing information to outsiders for reasons such as profit, personal gain or revenge. (Rindfleisch, 1997)

Security breaches from within secondary user settings involve uncontrolled secondary usage of patient information. In this scenario, a secondary user has a legitimate right to access patient data for a particular purpose. However, the secondary user employs the data for uses not envisioned on patient consent forms, such as for data

mining. Secondary users include insurers, employers, and others in the health services industry. Few controls are in place to ensure information is used only for authorized purposes. For example, self insuring employers are entitled to receive fully identified patient information for their employees to use to make sound benefit management decisions. An example of a security problem involving uncontrolled secondary usage of patient information would be if the self insuring employer then uses genetic test information to fail to promote or to fire an employee in order to avoid future medical costs. Outside intrusion into medical ISs involve someone outside the organization attempting to steal information, damage systems or disrupt operations. (Rindfleisch, 1997)

Information technology plays a significant role in developing methods to handle security, privacy, and confidentiality concerns. The three general classes of technological interventions to improve system security are deterrents, obstacles and system management precautions.

Deterrents depend on the ethical behavior of hospital personnel and provide reminders and oversight to reinforce hospital standards. Deterrents can be nontechnological or technological. The nontechnological deterrent of user education and technological deterrents of alerts and reminders are effective in reinforcing the generally high ethical standards of the majority of health care clinicians. The technological deterrent of an audit trail is also effective when its use is public knowledge. Obstacles directly control the ability of a user to get information with the goal of limiting access to information. They help ensure that users can only access information for which they have

a legitimate need, protect information against eavesdropping, and validate the origin and content of orders. Firewalls enforce manageable perimeters around distributed ISs. Rights management software involves segmenting and encrypting data. The software used to access the record is standardized and distributed from the information custodian. Users are granted access keys based on their identity and need to know. Obtaining the key serves as a basis for an audit trail and offers future possibilities of being used across institutional boundaries. System management precautions involve proactively examining an ISs to ensure that known sources of vulnerability such as viruses are eliminated. (Rindfleisch, 1997) Table 1 represents a summary of technologies applicable to information security management.

Intervention	Function	Example Technologies
<b>Deterrents</b>		
Alerts and reminders	Reinforce user ethics	Vendor specific
Audit trails	Document access/give alerts	Custom research systems and some vendors
<b>Obstacles</b>		
Authentication	Determine who is connecting	Accounts/passwords, kerberos, tokens (e.g. SecurID), public-key systems, biometric systems
Authorization	Define who can access what information	OS file and database vendor access controls, DCE access control lists
Integrity management	Ensure information content is as intended	Cryptographic checksums
Digital signatures	Validate notes and orders	Evolving standards
Encryption	Prevent eavesdropping	PGP, kerberos, DES, public-key systems, secure sockets
Firewalls and network service management	Define system perimeter and control means of access	Many vendors
Rights management tools	Control information distribution and access	IBM Cryptolopes
<b>Systems Management Precautions</b>		
Software management	Guard against viruses, Trojan horses, etc	Tripwire and controls such as loading of uncertified software
Systems vulnerability analysis tools	Detect unintended system vulnerabilities	SATAN, crack, National Computer Security Association

Table 1. Summary of Technologies in IS Security Management. (From Rindfleisch, 1997)

The first step in developing methods to handle security, privacy, and confidentiality concerns is to have an explicit policy from the HCO defining what is and what is not appropriate use of information. Simple, non-technical measures are appropriate to avoid accidental or curiosity driven disclosure of confidential information. Chief Information Officers have a number of technologies available in commercial systems or routine practice. Technologies such as audit trails can be used to curb insider curiosity and dissuade insider subordination. Currently deterrence and obstacles have provided little help in controlling security breaches by secondary users. Once the data has left the HCO and stored off site, the access and use controls are in the hands of the secondary user. As discussed above, rights management tools provide some promise for the future. (Rindfleisch, 1997) Table 2 relates the classes of disclosure threats to the available tools.

Threat	Principal Countermeasures
Insider Abuse	
Accidental disclosures	Education, alerts, reminders
Insider curiosity	Education, authentication, authorization, audit trail, rights management tools (future possibilities)
Insider subordination	Same as above
Secondary users	Rights management tools (future possibilities)
Outsider intrusion	All available obstacles and system management precautions

Table 2. Relation of Disclosure Threats to Security Technologies. (From Rindfleisch, 1997)

Ultimately the decision of what kind and how much security to implement is a management decision. As with all management decisions, functional benefits must be balanced with total costs and acceptable risks. Total costs include the cost of purchase and integration of security measures, the cost of management, operations and



maintenance of security measures, the cost of user time lost to satisfy security and the cost of user frustration with interfaces and procedures. CIOs will need to choose a set of non-technological and technological interventions that provide effective protection against perceived threats to system security at an acceptable cost.

## **B. CORE COMPETENCIES OF A CIVILIAN MEDICAL CHIEF INFORMATION OFFICER**

### **1. Introduction**

To develop a set of core competencies for a civilian medical chief information officer, the author uses the critical success factors described in the previous section of this chapter. The author develops a list of core competencies necessary to support each critical success factor as described in the Methodology chapter of this thesis. The core competencies necessary for a civilian medical CIO to be successful at meeting the critical success factors are technical competence, health care business competence, management competence, leadership competence, systems thinking competence, communication competence, and change management competence.

### **2. Technological Competence**

Technological competence is the primary core competency of a civilian medical CIO. The CIO is the custodian and manager of the IT asset. To manage an IT asset the CIO must understand its composition and characteristics, identify how it contributes to the

goals of the organization, and assess its performance. To accomplish these goals takes the intimate involvement of the CIO in technology and that takes technological competence.

To align an IS function and activities with the organizational strategy the civilian medical CIO must possess technological competence. To use the CAM requires continuously assessing seven components. Four of those seven components, external environment, emerging IT, IT infrastructure and IT strategy are impossible to accomplish without technological competence.

The CSF of strengthening the role of the CIO requires technological competence. If the CIO is to add value to the organization, to the executive team, and to the CEO he must be technologically competent. The CSF of creating, altering and managing IT assets requires technological competence in order to create an agile IT infrastructure, accurate, high quality data and IS staff expertise required in the civilian medical environment. In this environment, the management competence of a CIO can make or break careers and organizations. It is logical to assume that no CEO or executive team of any caliber will want a CIO that is not technologically competent as their technology adviser.

To make clinical ISs more useful and relevant to clinicians, the CIO again must be technologically competent. The problems of clinicians and computers are discussed in detail in the previous section of this thesis. The author suggests that the answer to many of the problems is more user involvement in planning, developing, and implementing ISs and in understanding how ISs cause social and organizational changes in the work place. Always understood in this answer is that someone in the organization must know

technology and its effects on the workplace. That someone may be the clinician, but it must be a technologically competent CIO.

If facilitating the transition to the IDN is a CSF and defining the infrastructure is one of the most important decisions a CIO makes, then a technologically competent CIO will make better infrastructure decisions than a non-technologically competent CIO. Also if developing methods to handle security, privacy and confidentiality concerns is a CSF of a civilian medical CIO, knowing the organization's IT, knowing security technology, knowing where to look in and out of technology areas for threats, and knowing what technology to apply and when to apply it are all essential for success in this area. A technologically competent CIO will be able to succeed at this CSF. A CIO not technologically competent will likely fail in this complicated area. Every one of the CSFs identified for a civilian medical CIO are achievable by a CIO with technological competence.

### **3. Health Care Business Competence**

Equally important to technological competence for a civilian medical CIO is health care business competence. Health care business competence requires knowledge of two unique but interrelated aspects of the health care field. These areas are the business aspect of health care and the clinical aspect of health care. Each of the two areas has its own knowledge base and language but both are an intimate part of the health care business environment. Knowledge and ability to communicate in each area is an essential part of the health care business competence.

The CSF of aligning IS function and activities with the organization's strategies requires that the CIO know the business. Four of those seven components of the CAM, external environment, mission, organizational infrastructure and business strategy are impossible to assess without health care business competence. Assessing the external environment requires both technological and health care business competence. A real understanding of the mission of the HCO is possible only by first understanding the health care business.

The health care business competence is essential to strengthening the role of the CIO. If IT and the CIO are the integrators of the COC, the CIO that has health care business competence will best understand how to use IT to enable the COC and the IDN. In a hospital environment the CEO and executive management team will most likely be physicians or health care administrators. To forge these essential bonds between the CIO and the CEO and the CIO and the executive team will require that the CIO speak the language of the CEO and the executive team. For the CIO to add value to the organization, strategically manage the IS function, realistically speak the language of the executives, and generally be a credible member of the executive team he must possess the health care business competence.

While a CIO does not specifically need health care business competence to manage the day to day operations of the IT assets, health care business competence is necessary to strategically apply that asset within the organization. To understand all the aspects of making clinical ISs more useful and relevant to clinicians, the CIO must speak the clinical

language discussed earlier and have an understanding of the clinical environment. Nothing upsets a clinician more than to have an administrator or a “techie” enter the clinical environment and dictate policy or “solutions” for perceived problems. That type of action has resulted in the rejection of ISs by clinicians in the past and is a part of the problem this particular CSF addresses. The CIO who possesses the clinical portion of health care business competence will understand this issue. The CSF of facilitating the transition to the IDN requires the same type of ability to speak and understand both health care business languages. Understanding is the first step in solving business problems.

The CSF of developing methods to handle security, privacy and confidentiality concerns requires a CIO to again have health care business competence. A CIO must be able to understand the security issues of the patient, the clinicians and the enterprise. There are legal, moral, ethical, and political ramifications of security in health care. The CIO with the health care business competence will understand all of those issues and will better evaluate the costs, risks and benefits of the health care security arena. Without health care business competence the CIO would have difficulty accurately prioritizing security issues in the HCO. Health care business competence is invaluable for a CIO and is involved with the accomplishment of every critical success factor.

#### **4. Management Competence**

The management competence concept has three aspects to it:

- financial management skills;
- customer awareness focus and skills;

- personnel management skills.

The first aspect involves skills and knowledge of the tools necessary to understand cost benefit analysis, return on investment, risk management, and performance and results based management kind of functions and analyses. This aspect of management competence enables the manager to effectively evaluate his area of responsibility in financial terms. The second aspect of management competence involves using the financial management evaluations discussed above to make strategic decisions. Customer awareness skills are necessary to this aspect of management competence. The third aspect of management competence deals with the skills to hire, evaluate, train, and develop personnel. This aspect of management competence deals with the personnel aspects of management. To have management competence means the CIO is proficient in all three areas.

A strategic focus is necessary to align the IS function with the organization's strategies. Since the CIO's management of the IT asset can often make or break a CEO and a company, management competence is necessary for successfully accomplishing the CSFs of strengthening the role of the CIO. Management competency is obviously critical to creating, altering and managing an IT asset. The CIO must exhibit the financial management skills, customer awareness skills and personnel management skills discussed above as well as delegation skills. The financial management skills discussed above are essential when dealing with the CSF involving developing methods to handle security, privacy and confidentiality. The decision concerning how much and what kinds of security

to implement is a management decision. Management competence is a core competency for a civilian medical CIO.

## **5. Leadership Competence**

What is leadership? It may be like beauty; that is leadership is in the eye of the beholder. Most people agree that an organization needs leadership. In the DON medical CIO survey to be discussed later in this thesis, one hundred percent of the respondents rated leadership as a necessary core competency of a Navy medical CIO. Drucker says that the only definition of a leader is "someone who has followers." (Drucker, 1996) Hammer says that "what a leader brings to an organization is strategy, motivation and integration." (Hammer, 1996)

The author uses the five characteristics of a leader developed by Bennis<sup>1</sup> to discuss leadership. The first characteristic of a leader is that he has a strong sense of purpose, a passion, and a sense of wanting to do something meaningful to make a difference. A leader can create a vision and share it. The second characteristic is that a leader is capable of developing and sustaining rich and trusting relationships. A leader has integrity and is caring and authentic with people. His followers do the right thing. The third characteristic of a leader is that he is a provider of hope and his followers have a sense that, whatever it is, they can do it. The fourth characteristic of a leader is that he keeps a balance in his life between work, family and outside activities. The fifth characteristic is

---

<sup>1</sup> Warren Bennis, the author of several books on leadership is a distinguished professor of Business Administration and founding chairman of the Leadership Institute at the University of Southern California.

that a leader has a bias towards action. Although not reckless, a leader does not hesitate to take risks. (Bennis, 1996) A leadership competence encompasses all of these five characteristics.

It requires all of the five characteristics of leadership to be able to be successful at each of the critical success factors identified for a civilian medical CIO. Each CSF requires that an assessment is made of the current situation, a vision of an idealized future state is created, and plans to migrate to the ideal future state are developed. The vision has to come from a leader. The CSF of strengthening the role of the CIO requires that a CIO have integrity in order to develop those one-on-one trusting relationships with the CEO and the members of the executive team. Personal integrity is also important when dealing with the clinical community as discussed in CSFs concerning making clinical IS useful and relevant to clinicians and facilitating the transition to the IDN. A strong sense of integrity is important in understanding the consequences of security and confidentiality of patient information. Personal integrity is a key feature of a leader and of the leadership competency.

## **6. Systems Thinking Competence**

Every one of the CSFs deals with a complex set of interrelated systems. To understand systems, one needs to understand the underlying patterns of the systems. Senge calls this "systems thinking" or "the fifth discipline" and it is one of his five basic learning disciplines (Senge, 1990).



Systems thinking is a discipline for seeing wholes. It is a frame-work for seeing interrelationships rather than linear cause and effect chains and seeing processes of change rather than snapshots. It involves understanding both reinforcing and balancing feedback processes and understanding delays. Reinforcing feedback process are the engines of growth. A good example is a snowball rolling down hill. Balancing or stabilizing feedback processes operate where there is goal oriented behavior. Your body's temperature regulation is a good example. If you are cold, your body closes your pores to retain heat. If you are warm you body perspires to cool you. To understand balancing processes you must discover the sources of stability and resistance. Understanding delays involves knowing that feedback processes contain interruptions in the flow of influence which can make the consequences of action occur gradually. Complex systems contain many combinations of reinforcing feedback, balancing feedback and delays. The goal is to understand the patterns of complexity. (Senge, 1990) The ability to understand the patterns of complexity is a core competency of a CIO in the complex worlds of information technology and health care. Without it he is likely to be spinning his wheels, chasing the wrong solutions.

To align IS function and activities with an organization's strategies requires understanding the patterns that hold the CAM system together. Strengthening the role of the CIO requires understanding the complex personal and professional relationships of the executive management team and the CEO. Creating, altering, and managing the IT asset means attempting to understand one of the fastest changing and the most complex fields.

The CSFs of making clinical ISs more useful to clinicians and facilitating the transition to the IDN involve the intersecting complexities of IT and health care. Getting a handle on all the possible security issues in IT and health care is also complex. The successful management of all of these CSFs is impossible without a systems thinking competence.

## **7. Communications Competence**

Good communications skills are essential for every executive and have relevance for each critical success factor. To align an IS function with the organization requires communication skill to assess the environment and to distribute and sell the CIOs vision of the technology portion of the strategic plan. Communication skills are necessary to develop a one-on-one relationship with the CEO and in developing partnerships with other members of the executive team essential for the CSF of strengthening the role of the CIO. Creating, altering and managing IT assets requires the ability to communicate inside the IS department and to communicate the department's goals and ideals to the rest of the organization. Dealing with clinicians, in making the clinical ISs more useful and relevant and in facilitating the transition to IDN, requires excellent communication skills. As stated previously, the clinical, business, and technology fields all have their own language, acronyms, goals, and ideals that create translational problems. One excellent way of bridging those translational gaps is with outstanding communications skills that start with knowing how to speak all of those "languages." Finally the security CSF requires superior communication skills to be able to explain and possibly defend a security plan to wary patients, staff, and executives.

## **8. Change Management Competence**

As stated in the introduction to this thesis, the rate of change in IT will accelerate as IT continues to evolve at a rate unsurpassed by any other technological change in recorded history (Hoffman 1994). The world of medicine is literally exploding with new and expanding technologies that are revolutionizing the delivery of health care. It seems as though almost everyone in business and government has some need for data from the health care world, either as patients, payers, or for research. The CIO is at the center of these colliding vortices and things are changing rapidly and in many dimensions. In order for the CIO to survive in this rapidly changing environment and to successfully meet his critical success factors the CIO must have change management skills.

Change management skills involve the ability to recognize change and its consequences, to plan change effectively and to manage change and its consequences.

The change management process has several aspects:

- setting goals and designing a desired future state;
- diagnosing the present condition in relation to future goals;
- defining the transition state and the activities required to meet the future state;
- developing strategies and action plans for managing the transition (Beckhard, 1987)

The main reason given for clinician avoidance of technology is too little clinician involvement in the development and implementation of clinical IT. Change management skills would have recognized this possibility and planned to overcome it. Aligning the ISs

function with the organization may require change in the IS department or in the business. Strengthening the role of the CIO in the organization means decreasing someone else's role in the organization. Altering the IT asset entails internal change in the IS department. Making clinical ISs more useful to clinicians and facilitating the transition to IDN will require change in the IS department and the clinical departments. Changing or implementing security procedures requires change for any number of systems and personnel. Change management skills would enable a manager to recognize and effectively deal with these situations. Change management skills are essential for the civilian medical CIO.

## **C. RESPONSIBILITIES OF A DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER**

### **1. Introduction**

According to Rockart, critical success factors are related to the structure of the industry of the executive, the organization in which the executive works, the environment and temporal factors. To use Rockart's model for developing a set of critical success factors for executives it is necessary to narrow the scope from a Department of Defense Chief Information Officer to a Department of the Navy Chief Information Officer. For the DON CIO the industry is the defense industry and the organization is the United States Navy that is part of the Department of Defense. The environment includes the current pressure to right-size the armed forces and all federal agencies and the need to fight one major theater war or two limited regional conflicts and perform operations other than war.

The author described temporal factors earlier in the setting that created the ITMRA mandate, in Chapter 2, Section C of this thesis. All four of Rockart's sources of CSF are in agreement in the crucial areas of funding and personnel. For the future, both the amount of money and the number of personnel in the DOD and DON available for supporting IT, are decreasing. At the same time, IT warfighting requirements are increasing. Using those factors as a basis, I will now define the responsibilities of the Navy CIO.

There are seven major responsibilities of a Navy CIO. Most respond to temporal factors and come directly from the ITMRA mandate and therefore have a basis in law. The rest come from the other three sources of CSFs discussed above. This is not unusual since the industry, the organization and the environment all work to shape this particular temporal factor. The six critical success factors for the Navy CIO are:

- develop and sell a strategic plan;
- implement an information technology architecture that supports the strategic plan;
- set goals for information technology within the Department of the Navy;
- manage and establish credibility for information resource management within Department of the Navy;
- increase the technological maturity of the Department of the Navy;
- participate and guide the Chief Information Officer council. (Frew, 1997)

## **2. Develop and Sell a Strategic Plan**

ITMRA mandates the development of a strategic plan so the DON CIO must be able to develop and sell an IM/IT strategic plan. The IT strategic plan for the Navy must align with the strategic plans of the Navy and the DOD and the IT strategic plan of the DOD. Performance measures must provide the basis for the strategic plan. To develop a strategic plan for IM/IT in the Navy, the DON CIO must be able to articulate a vision, put it in terms that are understandable to the people in the organization, develop a core group of believers and sell the vision while developing a critical mass. The leader of an organization must formulate and communicate a picture of the organization that everyone can understand and to which all can contribute. He must shape the attitudes and thinking of the people in the organization. Most people are not motivated solely for monetary reward but must be inspired by a meaningful vision of the significance of their work (Hammer, 1996). Selling the vision requires a CIO to consistently invest personal time in discussions that develop and test his vision (Earl, 1994).

The DOD provides guidance for the IM/IT strategic plan. The IM/IT strategic plan defines the missions, goals, and objectives of the organization and how IM/IT programs and initiatives support their accomplishment. The first step is in defining the mission of the IM/IT function within the organization. There are three sources for the IM/IT mission statement. They include the overall mission statement of the organization, policy directives and guidance from the organizational leadership, and external sources such as legislation and OMB directives. (Paige, 1997b)

From the mission statement, the strategic planner defines specific goals that must be achieved in order to accomplish the mission. These goals are at the next lower level of detail from the mission statement. They may be arranged according to the organizational structure, by functional area such as how IM/IT will support specific aspects of the organization's functions, by specific IM/IT functions such as infrastructure, security, and communications, or by a combination of these. The key is to ensure that each goal directly links back to the overall IM/IT mission and to the overall mission of the organization. All goals should be outcome based and a measurable outcome defined. (Paige, 1997b)

Objectives drive the process down to the next level of resolution. Specific, quantifiable and measurable outcomes that contribute directly to the achievement of the organization's IM/IT goals define the objectives. They may be tied to a specific IM/IT initiative or program, a specific level of compliance with standards or preferably measurable improvement in functional effectiveness or efficiency. (Paige, 1997b)

The final step is to identify the performance measures that will define accomplishment of each objective. Each performance measure has to answer the following questions:

- What is the purpose of the measurement?
- Who takes the measurement and how?
- Who uses the measurement and for what?
- What is the cost of the measure versus the value to the user?

- What tools and assistance are available to collect and use measurement data?
- What special provisions must be considered? (Paige, 1997b)

In IRM, technology trends can provide useful information for developing and IM/IT strategic vision and plan. Knowledge of new technology and its application to an organization is essential expertise for the DON CIO to possess. Knowing an organization's tolerance for change and when to schedule changes to new technologies are other essential skills for conserving the organization's resources. The DON CIO must be able to communicate the possibilities and limitations of new technologies to other senior managers and strategic direction to DON IT professionals. He must be able to thrive in a world where a "significant portion of IT resources inside the enterprise are under the administrative control of others." (Frew, 1996)

### **3. Implement an Information Technology Architecture that Supports the Strategic Plan**

One of the requirements of the Clinger-Cohen Amendment is for the CIO to develop, maintain and facilitate implementation of an integrated IT architecture (ITMRA, 1996). An IT architecture is the "set of design criteria, implementation rules and technical standards that governs the design, deployment and operation of all information technology and systems in an organization." (Hoffman, 1994) This definition emphasizes proactively managing IT functions as a whole, while also managing the development, operation and support of individual information systems. Building a comprehensive enterprise wide MIS is not practically feasible because it costs too much, takes too long



and does not meet the needs of the constantly changing environment of the DOD (Hoffman, 1994).

One concept of an architecture that supports the widely distributed needs of the DON is what Hoffman calls the application/infrastructure (A/I) architecture. This architecture divides the segments of IS into two parts; applications and infrastructure. Applications are systems that deliver the information needed to run an enterprise. They may support a business process or a functional organization but mostly likely they support both. Applications contain the elements of the IS that are unique to a business processes and activities. They are the property of the users, and users should build and manage them. Users are uniquely suited to best understand the needs of the business, know the organization's business rules and the business processes and comprehend the interrelationships of the business processes. (Hoffman, 1994)

Infrastructure in an A/I architecture consists of all facilities and programs that can support more than one activity or process. It includes all the resources used to construct, connect and support applications except what is unique to each application. Infrastructure contains four elements:

- the computer and communication network;
- data,
- technical tools and administrative procedures;
- people. (Hoffman, 1994).

The computer and communications network should support widely available broad bandwidth communication with the goal of universal connectivity and the capacity to support communication in any medium. Data should be managed with stable enterprise-wide data control processes. Data is included as part of the infrastructure to emphasize its effectiveness as being available to all applications and individuals who need it. Technical tools and administrative procedures, particularly establishing and maintaining standards, aid in the rapid delivery of high quality applications. (Frew, 1996) Talented people, who provide service to customers rather than systems to users, are needed to support the systems built by IT and act as consultants to users who build their own ISs (Hoffman, 1994). The development, implementation and maintenance of the infrastructure as a corporate wide resource is a responsibility of the CIO.

The DON CIO must be able to manage both a real and a virtual infrastructure. Management of a real network, where the CIO owns all the pieces such as an internal local area network is a straight forward concept. However it is not necessary to own things for them to be part of a corporate network and managed as a corporate resource (Emery, 1997). Increasingly direct ownership of network assets will eventually become vague and meaningless but the management of those functions is still vital. In the A/I architecture, future systems need to be able to take advantage of changing business rules and technological change without replacing infrastructure (Frew, 1996). Key to this concept is establishing a complete set of standards and providing effective, reliable operations. The DON CIO must understand and thrive in this environment.

#### **4. Set Goals for Information Technology Within the Department of the Navy**

ITMRA mandates that each agency CIO integrate IM/IT planning and management process with the business process, capital planning, and acquisition. Congress is demanding productivity improvements for each agency in return for resources. To do this the DON CIO must begin by setting IT goals within DON as a portion of the implementation of his strategic plan. In order to set these goals the DON CIO must have an understanding of the technological issues involved, the DOD acquisition process, the business processes in the DON, DOD and the private sector, people and change management skills, and management tools such as capital planning, return on investment (ROI) and performance and results based management.

The DON CIO is responsible for measuring the success of his IT procurements by focusing on performance and results to measure effectiveness and efficiency of the technologies. Performance goals must be benchmarked with comparable processes and organizations in the public and private sectors. This requires that the CIO be intimately familiar with other organizations that have comparable processes. He must develop a user focus to determine baseline work stations, tools and connectivity, common requirements and establish a plan and funding to meet the requirements (Langston, 1997b). This is a change in focus in a government agency not noted for its ability to quickly adapt to change. It requires that the CIO possess an understanding of personnel skills and the

factors involved in managing change in a complex environment. The goals he sets become the measures that will judge the CIO's performance.

#### **5. Manage and Establish Credibility for Information Resource Management Within Department of the Navy**

The Paperwork Reduction Act of 1995 requires the DON CIO to manage information resources to improve public access to information (Langston, 1997b). The Clinger-Cohen Amendment requires the DON CIO to assess agency personnel knowledge and skills in IRM and develop plans to address workforce IM/IT competency requirements. Satisfying these two requirements and providing a consistent and high quality product over an extended period of time will lead to the establishment of credibility in IRM within the DON. Good management, by properly distributing resources and overseeing the internal economy and business processes, is one of the keys to providing a consistent and high quality product. Because establishing credibility in IRM is partly political, the DON CIO must be politically aware of his environment and able and willing to act in a political manner to help establish this credibility. A DON CIO must have good management competencies and possess the traits of professional proficiency and personal integrity for his department to be credible within the DON and the DOD. (Frew, 1996)

#### **6. Increase the Technological Maturity of the Department of the Navy**

As noted in the introduction to section C of this Chapter, the number of personnel and the money for funding the DON in general and IM/IT in particular are steadily decreasing while IT warfighting requirements are increasing. Congress expects agencies

to cut IT costs five percent per year and to use IT to increase efficiency of operations five percent per year. In the environment described by the factors noted above, it becomes imperative for the DON CIO to increase the technological maturity of his organization. Technologically mature organizations are likely to take advantage of new technologies because their management is comfortable managing technology and the users are comfortable using IT (Sprague, 1993).

In Hoffman's A/I architecture discussed above, the DON CIO is responsible for developing, implementing, maintaining and managing the infrastructure and the users are responsible for managing and building the applications. To do this efficiently and effectively requires a mature technology. As the technology matures, it becomes easier and cheaper for an organization to take advantage of computer and telecommunication innovations and applications throughout the organization. Technology professionals must help users adapt to new technologies, use technology in innovative ways, understand and use technological tools, and build systems without IRM help. This requires that IRM staff have adequate infrastructures and support for those products and projects. (Frew, 1996) Technological maturity will aid in achieving these goals.

## **7. Participate in and Guide the Chief Information Officer Council**

Clinger-Cohen and President Clinton's Executive Order 13011 require the Department of the Navy Chief Information Officer participate in the Chief Information Officer council. Participation in a legislatively mandated council of peers requires

management and political competencies. The CIO council is an excellent forum for the DON CIO to work with the other CIOs to share best practices, lessons learned, and sponsor cooperation in using information resources. A subcommittee of the council developed a list of core competency areas necessary for a DOD CIO and as such took on oversight for the ITMRA mandated professional development of IRM skills of IT professionals.

#### **D. CORE COMPETENCIES OF A DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER**

##### **1. Introduction**

To develop a set of core competencies for a Department of Defense chief information officer the author uses the critical success factors described in the previous section of this chapter. The author develops a list of core competencies necessary to support each critical success factor as described in the Methodology chapter of this thesis. The core competencies necessary for a DON CIO to be successful at meeting the critical success factors are political competence, DOD business competence, communications competence, management competence, technological competence, leadership competence, and change management competence.

##### **2. Political Competence**

The DON CIO holds an appointed position in the United States government. This fact alone makes him a political being. To be in the position he holds, the DON CIO must

understand and thrive in the world of politics. Politics involves understanding and controlling power, influence, and authority. Political action takes place when an individual, recognizing that the behavior of others influences achievement of his goals, takes action against the others to ensure that he achieves his goals (MacMillan, 1976).

The CSF of developing and selling a strategic plan states that a DON CIO must be able to thrive in a world where he does not directly control the resources necessary to accomplish his goals. He must try to persuade those inside his organization to follow his plan but he may not have the ability to directly enforce his plan with the threat of withholding resources. Understanding and controlling power, influence, and authority are essential to be successful in this environment. Having a political competence will help the DON CIO be successful in this CSF.

The CSFs of implementing an IT infrastructure that support the strategic plan and setting goals for IT within the DON also require a political competence. The DON CIO must persuade the organization that his vision of an architecture is an acceptable one that will meet the user's needs. This occurs without any direct ability to enforce the DON CIO's vision and requires political competence. Likewise the goals for IT within the DON may be contradictory to what some users think the goals should be. A political competency will help to settle these issues.

The CSF of establishing credibility in IRM within the DON is partly political. The DON CIO must be politically aware of his environment and be able to use his political strength and competence to help establish this credibility. Finally, the CSF of participating

in and guiding the CIO council involves a group of political appointees acting on a federally mandated council to perform actions required by law. Although designed as a forum for sharing best practices and resources, practically each of the political appointees owes his allegiance to a different department, goal and benefactor. The politically competent CIO must be able to understand this environment and use his political competence to advance his organization in the spirit of sharing information and resources.

### **3. DOD Business Competency**

Knowing your business environment is a key to success in any field. Knowing an organization's purposes, structure, reward system, leadership approach, relationships between people, relationships between business units and helpful mechanisms such as procedures, policies, and systems and how they fit together will provide the DON CIO an understanding of the environment (Weisbord, 1976). The federal government operates its business very differently than the private sector. Although it is attempting to change and become more like the private sector, the federal government is essentially a not for profit organization with its own rules concerning budgeting, accounting, and acquisition. Working in the federal sector requires that the DON CIO be familiar with the Planning Programming and Budgeting System of the federal government and the Program Objective Memorandum system to obtain funding for large systems. It also requires a knowledge of federal accounting principles, policies and procedures and acquisition regulations such as FARA. Since the federal government is a not for profit organization, until recently many of the concepts from private industry, such as profit and loss statements, were unknown to



federal employees. Much of the overspending in federal programs occurred because the federal system formerly did little to incentivize its employees to avoid waste. After all, there is no profit sharing in a not for profit organization. ITMRA is the reason the DON has a CIO. The successful DON CIO must be able to understand ITMRA and avoid the problems that produced it. This requires a DOD business competency.

The DON CIO must understand the business principles of the federal government to succeed in his CSFs. The CSF of developing and selling a strategic plan for the DON will happen with DOD guidance. A DON CIO who does not understand the DOD business might fail from the outset. Implementing an IT architecture for the DON will be done in compliance with the infrastructure of the DOD, the Defense Information Infrastructure guidance. Acquiring the pieces for architecture requires knowledge of the federal acquisition process. Setting goals for IT within the DON requires a knowledge and competency in the DOD acquisition process and the business processes of the DON and DOD. The CSF of managing and establishing credibility for IRM within the DON requires understanding, the Paperwork Reduction Act of 1995, FARA and ITMRA. Clearly a DOD business competency is essential for the DON CIO to succeed.

#### **4. Communications Competence**

Good communications skills are essential for every executive and have relevance for each critical success factor. To develop and sell a strategic plan and to set goals for IT within the DON requires buy-in from the entire organization. The DON CIO must articulate a vision and goals and communicate a picture of the organization that all can

understand and to which all can contribute. Goals and vision have little value unless shared and adopted. To implement an IT architecture requires coordination across the enterprise. Communication skills aid this coordination process. Managing and establishing credibility for IMR within the DON requires a communication competence to spread the word concerning the importance of IRM, to educate the work staff on IRM and then to tell the world about the DON's IRM abilities when they are established. Good use of communications will develop the comfort level of managers and users discussed in the CSF of increasing the technological maturity of the DON. Good communications skills will aid end users in adapting to new technologies. Finally the CSF of participating and guiding the CIO council, demands sharing best practices and information resources inside the council. This CSF will not come to fruition without communications skills and the communication competence.

## **5. Management Competence**

As stated in section B of this chapter concerning the management core competency of a civilian medical CIO, there are three aspects to management competence: financial management skills, customer awareness focus and skills, and personnel management skills. To have management competence means the CIO must be proficient in all three areas.

The strategic plan discussed in the CSF of developing and selling a strategic plan, must be based on performance measure, requiring the financial management competence. Implementing an IT architecture that supports the strategic plan must be customer focused, requiring management competence. Setting goals for IT within the DOD must be

focused on productivity improvement in the agency using performance and results based management. This cannot be accomplished without the DON CIO having a management competence. The CSF of managing and establishing credibility for IRM in DON concerns assessing agency personnel knowledge and skills in IRM and developing plans for the professional development of the agency personnel. The information resources management function is the financial portion of management competence. Increasing the technological maturity of the DON is a key management issue. Management competence is clearly a core competency of a DON CIO.

## **6. Technological Competence**

As discussed in section B of this chapter, technological competence is the primary skill required of a CIO. To be successful at each of the CSFs mentioned the DON CIO must understand the technology and its management. Each is about some aspect of technology. Developing and selling a strategic plan concerning IM/IT and implementing an IT architecture that supports the strategic plan will not occur without a knowledge of technology. Knowledge of new technology and its application to the business is an essential expertise for the DON CIO to possess. To set goals for IT within the DON requires a firm understanding of technological issues. To manage and establish IRM in the DON and increase the technological maturity of the DON, the CIO must have an overview of the technologies of the DON. Finally the CIO council objectives all deal with technology issues. Every one of the CSFs identified for a DON CIO is requires a CIO with technological competence.

## **7. Leadership Competence**

Section B of this chapter discusses aspects of leadership. Leadership skill and abilities are essential to successfully accomplish each of the critical success factor goals. Developing and selling a strategic plan and setting goals are a leader's responsibility. In order to implement an IT architecture, a vision of what that architecture looks like and how it works is essential. Vision is mandatory for establishing credibility for IRM in DON and increasing the technological maturity of DON. Then the vision must be communicated to all and work must start to realize the vision. None of this can occur without inspired leadership. The DON CIO must be a leader and must have leadership as a core competency to be successful.

## **8. Change Management Competence**

Section B of this chapter discusses change management skill as essential in the IT environment. The DON is changing, getting smaller in personnel and in funding. These changes require careful consideration of many aspects of change management skills, particularly planning change and the effects of change on the organization. The concept of a DON CIO is a change in itself. Each of the critical success factors identified for a DON CIO involves some type of fundamental change. Before ITMRA, the DON did not have a strategic plan or goals for IT based on performance. Until recently, the need to integrate DON's IT architecture with the DII and the National Information Infrastructure was not understood. Information resource management did not occur in the DON before ITMRA and, although there was a recognized need by some in DON to increase its technological

maturity, it was not a widely held view. Also the CIO council did not exist until ITMRA. Much is changing in the DON IT world, and much will continue to change. In order to be successful a DON CIO must have change management as a core competency or he will repeat the failures of the past.

## **E. SURVEY OF NAVY MEDICAL CHIEF INFORMATION OFFICERS**

### **1. Introduction**

The author conducted a survey of Navy medical CIOs at the DON CIO Conference/CHIME "Information Management Executive Course," described in the "Discussion of Survey Methodology" section in Chapter 3. The survey was conducted at the end of the second day of the first week of the course, prior to the CHIME course, to avoid the possibility that the CHIME course may have influenced the results of the survey. Although the survey contained a letter of introduction, the author was present to answer questions. The only questions asked concerned clarification on the difference between a core competency and a skill.

Twenty of twenty-one possible respondents returned the survey. The survey asked several demographic questions, questions to determine if the respondents were CIOs and presented a list of possible core competencies of a DON medical CIO. The list of possible core competencies was gathered from lists in several textbooks (Frenzel, 1992) (Sprague, 1994) (Palvia, 1992), the DOD CIO's Clinger-Cohen education and training program (Paige, 1997a), the Information Resource Management College's CIO certification

program (IRMC, 1997), CIO position descriptions (Gartner, 1997) and the CHIME course subject areas (CHIME, 1997). The author alphabetized the list of core competencies to avoid influencing the respondent's choice. A copy of the survey appears as Appendix B and a copy of the results of the survey appears as Appendix C.

## **2. Demographics**

The demographics indicate respondents are experienced IS/IT professionals. The respondents ranged from 30 to 52 years in age with a mean age of 37.5 years. One respondent failed to provide his age. Seventy-five percent of the respondents were male and twenty-five percent were female. Their years of IS/IT experience ranged from four to twenty years with a mean of 10.95 years. Their years of DOD IS/IT experience ranged from two to twenty years with a mean of 10.35 years. There were two civilian respondents with GS12 rank while the military respondents consisted of one O2, thirteen O3s, three O4s and one O5. The military respondents' years of military experience ranged from nine to nineteen years and averaged fifteen years. The civilian respondents possessed no prior military experience.

## **3. Determining if Respondent is a Chief Information Officer**

Burbridge and Boyle developed a matrix that classifies an IS executive based upon his responsibility for technology and reporting level within the organization (Burbridge, 1994). Figure 3 is the author's modified version of Burbridge and Boyle's matrix.

Responsibility For Technology	Broad	<u>Emerging CIO</u>  6 Navy medical CIOs	<u>CIO</u>  6 Navy medical CIOs
	Narrow	0 Navy medical CIOs  <u>Data Processing Manager</u>	0 Navy medical CIOs  <u>Start-up Business</u>
		Not ESC Member Low (DFA)	ESC Member High (CO)
Reporting Level Within the Organization			

Figure 3. Technology / Reporting Level Matrix. (After Burbridge, 1994)

Individuals in the upper right hand quadrant of the matrix have a broad responsibility for technology and high reporting level and are fulfilling the role of CIO within their organization. Those in the upper left hand corner of the matrix possess a broad responsibility for technology, low reporting level and are emerging CIOs. Individuals in the lower left hand corner of the matrix have a narrow responsibility for technology and low reporting level, are referred to as data processing managers and not considered to be CIOs. Those in the lower right hand corner of the matrix are involved in a start-up business and also not considered CIOs. No job title is linked to those in a start-up business.

For the purposes of this thesis, the twenty respondents were further subdivided into two groups. Group A consists of twelve individuals. Eleven of those individuals work in a hospital and their job responsibilities correlate to a CIO in a HCO. The other

individual works for DOD Health Services in a Tricare region. His job responsibilities also correlate to a CIO in a HCO. Group B consists of six individuals whose job responsibilities are in support activities at NMIMC and two individuals who are graduate students. Group B individuals could not be CIOs. The individuals in Group A are the focus of the remainder of this discussion.

Questions 10 through 13 of the survey are designed to measure an individual's responsibility for technology within their organization. The author uses a five point Likert scale with one representing high responsibility, three representing medium responsibility and five representing low responsibility for four different aspects of technology management. The four aspects of technology management are:

- managing the technology of the organization;
- managing the organization's technological development;
- managing the maintenance and operations of IT systems;
- planning the organizations future IS/IT needs.

Appendix B contains a copy of the survey. Table 3 represents the results of the survey.

Using the mean scores as indicators, CIOs number one to eleven all indicate they have a high responsibility for technology in their organization. CIO number twelve has a mean of 2.5 with three representing medium responsibility for technology. His low score in "Maintenance and Operations" stems from the fact that he has no responsibility for maintaining any information systems. All of these CIOs would then be in



one of the upper two quadrants of the Technology / Reporting Level Matrix depicted in Figure 3.

CIO	Managing Tech	Tech. Development	Maintenance & Ops	Planning	Mean
1	1.00	1.00	1.00	1.00	1.00
2	1.00	2.00	1.00	1.00	1.25
3	1.00	1.00	1.00	1.00	1.00
4	1.00	1.00	1.00	1.00	1.00
5	2.00	1.00	1.00	1.00	1.25
6	1.00	1.00	1.00	1.00	1.00
7	1.00	1.00	1.00	1.00	1.00
8	2.00	3.00	1.00	1.00	1.75
9	1.00	1.00	1.00	1.00	1.00
10	1.00	1.00	1.00	1.00	1.00
11	1.00	1.00	1.00	1.00	1.00
12	3.00	1.00	5.00	1.00	2.50

Table 3. CIO's Responsibility for Technology Management

In the DON medical environment there are two indicators of reporting level within the organization. One indicator is the CIO's reporting senior while a second indicator is membership on the command's Executive Steering Committee (ESC) or senior leadership committee. Although seven of the Group A individuals carry the title of CIO, only one individual reports to the Commanding Officer (CO) while one reports to the Executive Officer (XO). The other ten individuals report to the Director for Administration (DFA). The individuals reporting to the CO and XO are both members of their command's ESC. These two are classified as CIOs. Of the other ten individuals, four are members of their commands ESC and are also be classified as CIOs. The other six are "Emerging CIOs." Four of the seven individuals in this study who have the title of CIOs are also "Emerging CIOs "

#### **4. Core Competencies**

The author listed 53 possible core competencies and seven spaces labeled "other \_\_\_\_\_" for the respondents to add other core competencies. For the purposes of this thesis, the author assumed that a core competency would pass the test if a majority (greater than fifty percent) of respondents indicated "yes" to the core competency on the survey form. All respondents' responses were considered because the respondents were identified by NMIMC as being CIOs or potential CIOs when they were invited. Even though only six of the respondents were identified as CIOs and six as emerging CIOs, the remaining eight individuals could likely function as CIOs in their next command and may have performed CIO duties at their last command. The usual rotation in the DON medical IS community is one tour of duty at NMIMC followed by a tour at a hospital command. The demographics section of this chapter indicates that the personnel in the survey are experienced IS/IT professionals.

A majority of the respondents identified 36 of 53 core competencies as necessary for a DON CIO to possess to be an effective member of the executive team. Appendix D is a graphical representation of the percentage of respondents who selected each core competency. Every respondent identified communication skills and leadership as core competencies. Ninety percent of the respondents identified the core competencies of customer awareness, knowledge of the health care business, life cycle management, partnership and team building, and planning as necessary core competencies. Project management skills and vision were identified by eighty-five percent of the respondents

while acquisition knowledge, benchmarking, capacity planning, change management, information resource management, staff development, strategic management, and technology integration skills were named by eighty percent of the respondents.

Seventy-five percent of the respondents chose baseline assessment/analysis, business process reengineering/improvement, knowledge of computer standards, contingency planning, contracting knowledge, cost-benefit analysis, performance measurement, return on investment, and the skills associated with making a source decision by comparing the benefits of making versus buying as necessary core competencies of a DON medical CIO. Risk analysis knowledge and staff evaluation skills were named by seventy percent of the respondents while sixty-five percent chose capital investment and planning, process quality improvement, risk management and technological competence as core competencies. Sixty percent of the respondents named knowledge of best practices, IS development and implementation, and organizational development as necessary core competencies. Finally fifty-five percent of the respondents chose organizational performance as a necessary core competency of a DON medical CIO.

## **F. CORE COMPETENCIES OF A NAVY MEDICAL CHIEF INFORMATION OFFICER**

### **1. Introduction**

The environment of the Navy medical CIO is a combination of the environments of a civilian medical CIO and the DON CIO plus the Navy medical CIO's operational responsibilities. The Navy medical CIO works in a situation analogous to the civilian

medical CIO. He faces all the duties and responsibilities that his civilian counterpart faces involving technology and the health care business, with two major exceptions. The exceptions are the areas of major ISs development and the active duty Navy medical CIO's operational responsibilities.

In the civilian medical setting, the CIO is responsible for purchasing and developing major administrative and clinical technologies and information systems. Most of the enterprise-wide decisions for major administrative and clinical systems for Navy medicine occur at higher levels of the Navy and DOD. To ensure enterprise-wide coordination, the Department of Defense maintains the office of Assistant Secretary of Defense for Health Affairs (ASD(HA)) that is responsible for oversight on medical issues in the DOD. Decisions concerning enterprise-wide technologies are made in a tri-service environment, with ASD(HA) oversight. Responsibilities for developing programs are distributed to the military services along product lines. Each service has administrative responsibility for developing and revising an entire product line of ISs but the development is done using input and personnel for all three services. Currently, each service is responsible for most of the local support for its information systems.

Active duty Navy medical CIOs have operational responsibilities that the civilian CIOs does not have. A Navy medical CIO's billet is tied to an operational responsibility. Whenever called upon, the active duty Navy medical CIO must be prepared to deploy to a fleet hospital or hospital ship. If deployed, the CIO must have systems in place to leave

the responsibility for information management at the HCO to an activated reservist or civilian personnel. Civilian medical CIOs do not have operational responsibilities.

The Navy medical CIO works in the same federal government environment as the DON CIO described earlier in this thesis, although at a lower level in the DON organization. The Navy medical CIO needs all of the knowledge and skills of the DON CIO concerning DOD budgeting, acquisition and finance.

Core competencies are proficiencies that a CIO must have if he is to be successful. The lists of core competencies developed by this author for the civilian medical CIO and DON CIO are almost identical. Since the Navy medical CIO has similar job responsibilities to the civilian medical CIO and the DON CIO, the Navy medical CIO's core competencies are also similar. The author makes the case that the core competencies of a Navy medical CIO are a combination of the two lists. Figure 4 illustrates the formation of the Navy medical CIOs core competencies. The resulting Navy medical CIO core competencies includes the common core competencies of leadership competence, communications competence, technological competence, management competence, change management competence, the combined category of DOD health care business competence, and the individual core competencies of political competence and systems thinking competence. Each of these competencies must be present in the Navy medical CIO or he will not be an effective and successful CIO. To be an expert technologist without all of the other seven competencies would render the CIO unsuccessful.

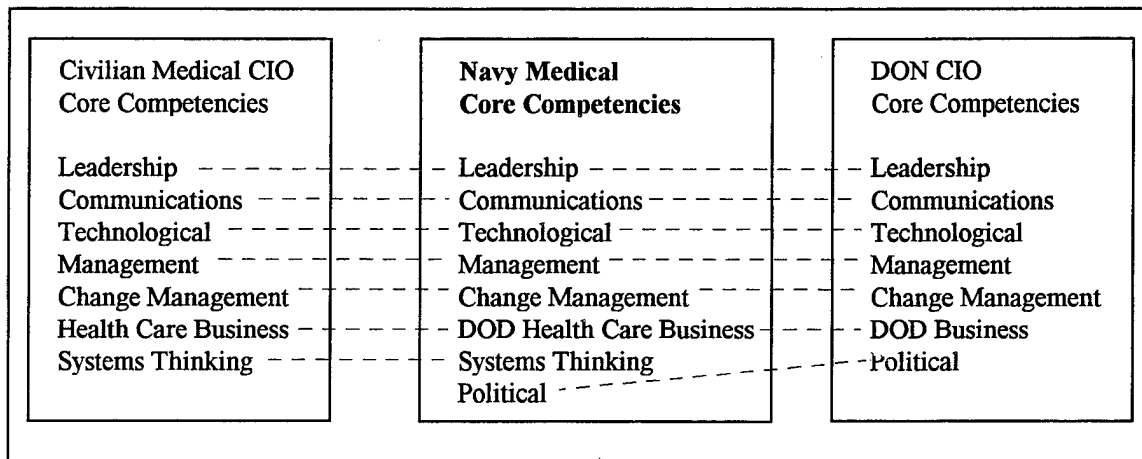


Figure 4. Formation of Navy medical CIO's Core Competencies.

## 2. Leadership Competence

Leadership has four tasks. They are defining purpose, embodying purpose in programs, defending institutional integrity, and ordering internal conflict. Defining purpose involves assessing the organization to define its true responsibilities. Embodying the purpose in programs concerns building the responsibilities of the organization into its structure so that the leader can expect reliable execution and clarification in policy. Defending the institutional integrity involves maintaining the values of the organization when necessary. Ordering internal conflict involves maintaining a balance of power within the organization that enables the organization to maintain its commitments. (Selznick, 1957)

The importance of leadership as a core competency was articulated earlier for the civilian medical CIO and the DON CIO. Leadership in a core competency for Navy medical CIOs for all the same reasons. It may even be more important for the active duty Navy medical CIO, since he may be called upon to leave the hospital for extended periods

of time if ordered to deploy. The active duty CIO must prepare his department for that eventuality. A good leader will be able to embody the purpose of his job functions in the structure and policies of his department to insure that the purpose continues when he is away. In the author's survey of Navy medical CIOs, one hundred percent of the respondents chose leadership as a core competency. Leadership was only one of two core competencies chosen by every respondent. Eighty-five percent of respondents chose vision and eighty percent chose strategic management and planning as core competencies. Vision and strategic management and planning are part of the leadership competence. The results of the survey may reflect the military's emphasis on the importance of leadership or it may reflect that effective leadership is essential in a military environment. Either way, leadership is a core competency of a Navy medical CIO.

### **3. Communication Competence**

Good communication skills are essential for every executive, including the Navy medical CIO. In the survey of Navy medical CIOs, one hundred percent of all respondents chose communication as an essential core competency. The communication competence concerns how well the CIO can convey information concerning IT issues to the organization. The CIO must be able to explain IT issues in the language of the user. The Navy medical CIO not only has to speak the languages of technology, clinical health care and business health care of the civilian medical CIO but must also be fluent in DON and DOD languages. Being able to relate technology concepts in each of those languages is a requirement for success.

The IS department no longer can live alone in the basement. Several Navy medical CIOs commented that explaining technology issues to people at various levels of the organization is one of their primary duties. Navy medical CIOs say they provide this service on a daily basis. Being able to discuss the advantages of using technology and other key technology concepts with the Commanding Officer, the Executive Steering Committee and within the IS department, requires well-developed communication skills. The personnel in the organization demand that the IS department assists in every aspect of planning and effectively managing the organization and its assets. This can only be accomplished if the organization's chief technologist can communicate to all who need to hear the word, making communications a core competency of a Navy medical CIO.

#### **4. Technological Competence**

Technological competence is a core competency of a Navy medical CIO. The CIO is the custodian and manager of the IT asset. To manage the IT asset, the CIO must understand its composition, characteristics, identify how it contributes to the goals of the organization, and assess its performance. To accomplish these goals requires the intimate involvement of the CIO in technology and that takes technological competence.

This is not to say that the Navy medical CIO, or any CIO, needs to know the intimate details of every technology. He does need an overall understanding of the technology and how it applies to his business. In order to create the agile IT infrastructure, accurate, high quality data and IS staff expertise required in the medical environment, the CIO must have a solid background in IT both from the standpoint of



educational background and from practical experience. An educational background in computer science or information technology management firmly grounds the CIO. Practical experience provides the CIO knowledge concerning the real world environment of IT. Each is an indispensable part of technological competence.

Clearly technological integration is important for Navy medical CIOs. In the survey, sixty percent listed IS development and implementation as a core competence, sixty-five percent listed technological competence, seventy percent listed knowledge of computer standards, while eighty-five percent listed technology integration skills as a core competency.

One of the critical aspects of technological integration is keeping up on new technologies. In early 1995, before it gave up counting because of sheer volume, Ernst & Young LLP estimated that 8,000 new software, hardware and information related products were released into the market every month (Bresnahan, 1996). This growth has only accelerated. Navy medical CIOs state that keeping up with new technologies is one of their most difficult responsibilities. The Navy medical CIO must be able to scan the market for new technologies and know how and when to apply them. This takes a combination of technological competence and health care business competence.

## **5. Management Competence**

As stated in section B of this chapter concerning the management core competency of a civilian medical CIO, there are three aspects to management competence: financial

management skills, customer awareness focus and skills, and personnel management skills.

To have management competence means the CIO must be proficient in all three areas.

The Navy medical CIO needs management competency to be successful. He is the department head and manager of the IS function in his hospital. Several Navy medical CIOs state that the Commanding Officer and members of the Executive Steering Committee judge the Navy medical CIO on how well the IS function in the hospital responds to its customers' needs. In the survey conducted for this thesis, the majority of respondents chose several topics as core competencies of a Navy medical CIO that have a management focus. The topics of baseline assessment and analysis, benchmarking, best practices, business process reengineering, capital investment and planning, capacity planning, contingency planning, cost benefit analysis, information resource management, lifecycle management, performance measures, planning, risk analysis, risk management, return on investment, source decision (make versus buy decisions), and strategic management all concern the first management aspect of financial management. Customer awareness is the second aspect of management and ninety percent of the respondents chose it as a core competency. The majority of respondents chose the topics of organizational development, organizational performance, staff development, and staff evaluation as core competencies. These topics all relate to the personnel aspect of management. The respondents of the survey view management in all its aspects as a core competency of a Navy medical CIO.

## **6. Change Management Competence**

The author has made a strong case that change management is a core competency of a civilian medical CIO and a DON CIO. Eighty percent of the respondents to the survey conducted for this thesis chose change management as a core competency. The worlds of technology and DOD health care are changing at unprecedented rates. Special skills are needed to plan and manage change, and its consequences, for the enterprise and its people. Change management is a core competency of a Navy medical CIO.

## **7. DOD Health Care Business Competence**

Whatever type of business a CIO's organization is in, the successful CIO must have a working knowledge of that business in order to apply technology to improve it. Earlier in this thesis, the author developed a strong case for the civilian medical CIO to have health care business as a core competency. Similarly he made a strong case for the DON CIO to have DOD business knowledge and a core competency. The Navy medical CIO lives in both worlds and needs both skills. The survey of Navy medical CIO validates this fact.

In the survey, ninety percent of the respondents rated health care business knowledge as a core competency. Although the survey did not list DOD business knowledge as a possibly core competency, it did list several possible core competencies that speak to the area of DOD business knowledge. These include acquisitions, contract management, and project management. Eighty-five percent of the respondent chose acquisition as a core competency, seventy-five percent chose contract management as a

core competency and eight-five percent chose project management as a core competency. The respondents recognized the fact that to be successful in Navy medicine, the CIO must understand technology and the business.

The environment of Navy and DOD medicine is changing with the advent of Tricare, DOD's managed care plan and DOD(HA) mandated capitation funding scheduled to begin October 1, 1997. The Navy hospital will be one of many choices that dependents and retirees can choose as their care manager. In order to compete in this new environment all executives of the Navy medical facility, including the Navy medical CIO, must have an understanding of the health care business. In an information intensive environment like health care, the development of a successful business strategy can only occur with the assistance of the organization's chief technologist. DOD health care business competence represents a combination of the health care business competence discussed for the civilian medical CIO and the DOD business competence discussed for the DON CIO. The competence recognizes the needs of the Navy medical CIO to be fluent in both areas. His business is DOD health care.

#### **8. Political Competence**

The Navy medical CIO is an employee of the federal government. He serves at discretion of the President of the United States of America. As difficult as it is to believe, the federal government in general and the United States Navy in particular are political entities. The Navy medical CIO must be able to thrive in a world where he does not directly control the resources or the organizational power necessary to accomplish his

goals. Most of the decisions on major information systems occur at a level far above the Navy medical CIO. Unfortunately the author's survey did not provide political skills as a core competency choice. Political skills did not appear as a core competency in any of the literature used to prepare the survey. However in the survey, four of the seven or fifty-seven percent of the individuals who hold the title of CIO at their commands had a low reporting level within the organization. Also in the survey, although twelve of the respondents had similar job characteristics and were the senior IS/IT person on staff, five of the twelve or forty-two percent did not have the title of CIO. Only fifty percent of Navy medical CIOs are CIOs by the definition in this study. The others are classified as "Emerging CIOs." Until all the "Emerging CIOs" actually become CIOs, a political competence is a core competency of a Navy medical CIO to be an effective member of the management team.

## **9. Systems Thinking Competence**

The Navy medical CIO must deal with a complex set of interrelated systems. These systems include information systems, the continuum of care, and the integrated delivery network. To understand systems, CIOs need to understand the underlying patterns of the systems. Systems thinking is a discipline for seeing wholes. It is a frame-work for seeing interrelationships rather than linear cause and effect chains and for seeing processes of change rather than snapshots. Complex systems contain many combinations of reinforcing feedback, balancing feedback and delays. The goal is to understand the patterns of complexity. (Senge, 1990) In order to understand complex systems, one must understand

the patterns that hold them together. When a change occurs in one part of the system, it will be felt in other parts of the system. Understanding the patterns that hold systems together will allow the Navy medical CIO to know the effects of change before they occur and better plan and manage a system and its changes. Systems thinking is a core competency of a Navy medical CIO.

#### **G. SKILLS NEEDED BY A NAVY MEDICAL CHIEF INFORMATION OFFICER**

Recall that a core competency is proficiency that a CIO must have if he is to be successful. A core competency can be contrasted with a skill. The true core competency is essential to be successful while a skill is nice to have. Without the skill a person can still succeed as a CIO. Skills needed by a Navy medical CIO are derived from the core competencies of a Navy medical CIO.

From the leadership competency come the two related skills of developing and selling a vision and strategic management and planning. From the communications competence come the oral speaking skills, writing skills, presentation skills and listening skills. Skills from the technological competence include IS development and implementation, knowledge of computer standards, technological integration skills, data managing skills, network management skills and educational skills.

There are a number of skills that are part of the management core competency. The skills include all of the business and finance related skills connected with managing projects and resources. Many were picked by the majority of Navy medical CIO as

important to have for the CIO to be an effective member of the executive team. They are baseline assessment and analysis, benchmarking, best practices, business process reengineering, capital investment and planning, capacity planning, contingency planning, cost benefit analysis, information resource management, lifecycle management, performance measures, planning, risk analysis, risk management, return on investment, source decision (make versus buy decisions), and strategic management. Part of management competence is the skill of customer awareness. Personnel type skills include organizational development, organizational performance, staff development, staff evaluation, team building, and personnel motivation skills.

Skills involved in the change management include the skills to recognize change and its consequences, planning skills, and personnel skills to deal with the results of change. The DOD health care competence includes acquisitions skills, contract management skills, and project management skills from the DOD portions of this competence. The health care side presents the skills of marketing and integration skills. Skills involved in the political competence are analytical skills, the management of power, and the exercise of influence and authority. Finally systems thinking involves integration skills, observational skills, and analytical skills.

## **H. MEASURES OF EFFECTIVENESS OF NAVY MEDICAL CHIEF INFORMATION OFFICER**

### **1. Current Measures of Effectiveness for Navy Medical Chief Information Officers**

In June of 1997, the author had several interviews and conversations over a twelve day period with twenty-one former, current and potential future Navy medical CIOs. One of the purposes of these discussions was to determine what measures of effectiveness are currently being used to judge the Navy medical CIO's contributions to the executive management of their organization. These discussions led to a consensus description of the current situation.

Currently, the effectiveness of Navy medical CIOs is measured by how well they know their systems, keep them running, and manage their resource under budgets. They measure their systems by how quickly they can respond to user questions and problems. Users want a system that is always available and expect that the day to day operations of their systems will run smoothly. They want to be able to read their e-mail and access clinical and administrative systems whenever they need them. System down time is a measure of a Navy medical CIO's effectiveness. Keeping ISs running concerns how quickly an IS department can recover after a system failure. The MOEs of system down time and recovery time are part of the CIO's technological competence. The third attribute of managing resource under budgets is the financial management measure of effectiveness. The percentage under budget is a MOE of the Navy medical CIO.



According to the survey conducted for this thesis, eighty-three percent, of current Navy medical CIOs, report to the Director for Administration. The DFA concerns include users' satisfaction with the IS department and the CIO coming in at or under budget at the end of the year. According to the Navy medical CIOs interviewed for this thesis, DFAs give little thought to prospective MOEs in the six other competency areas discussed in this thesis.

Navy medical CIOs interviewed for this thesis expressed a strong desire to get a seat at the executive table. Based on the survey developed for this thesis, only fifty percent of the those currently serving in Navy medical CIO positions sit on their command's ESC. They felt they had much to add to strategic discussions and were not currently represented well at the ESC level. Fifty percent of Navy medical CIOs report to the DFA who represents their department on the ESC. One Navy medical CIO suggested that the DFA does not adequately represent the strategic aspects of IT because the CIO is only one of many responsibilities of the DFA. Another said that the DFA often wants credit when the IS department succeeds but does not want any involvement in IS department failures. Many crises are avoidable if the CIO is on the ESC, another Navy medical CIO said. For example, she continued, sometimes snap decisions are made with the wrong or no information because ESC members do not know that good information is available. Several Navy medical CIOs expressed the opinion that to clearly articulate the benefits and needs of IT for the organization and have a real impact in the understanding of the ESC, the Navy medical CIO must be a member of the ESC. However, often in the

military, rank is an important qualifier for ESC membership. The majority of Navy medical CIOs are junior officers.

## **2. Measures of Effectiveness of Civilian Medical Chief Information Officers**

The author interviewed several current or past civilian medical CIOs and CEOs who were instructors at the CHIME "Information Management Executive Course." They include:

- Dr. James Martin currently President of a health care software development and consulting firm;
- Dr. John Glaser currently Vice President and CIO for Partners Health Care System INC. and the founding chairman of CHIME;
- Mr. Rick Skinner currently CIO for the Provident Health System and a retired Army officer;
- Mr. David E. Garets currently research director for the Gartner Group and a former CIO;
- Dr. William Bria M.D. currently Medical Director of Clinical Information Systems for the University of Michigan;
- Mr. Stephen Ummel currently National Advisor on Integrated Delivery Systems for Ernst & Young LLP and former CEO and chairman of the board of several health systems organizations;

- Mr. G. Ward Keever currently CIO for the University of Pennsylvania Health System;
- Dr. Alan Dowling currently partner of Global Health Care Consulting for Ernst and Young LLP a former CIO and a Colonel in the Air Force Reserve.

Several of these experts declared that CIOs are measured every day by their customers, supervisors, and fellow executives. The traditional evaluation measures like down time and system recovery time are being augmented with performance measures that are hard to quantify but known to other executives. With every conversation with the CEO or other executive, someone is making an evaluation on the CIO's performance. Research has shown no evidence that CIOs higher up in the organizational chart perform better than those lower down, but successful CIOs found a way to build relationships with top executives (Earl, 1994). The experts also defined certain intangibles by which the CIO is measured. They include such things as the ability to explain IT terminology to executives or other users and the ability of the CIO to mix well with board members (Glaser, 1997b). These are intangibles needed by every executive, not specific to the CIO. In civilian medical environment, CIOs are not judged by the work they do as much as by the relationships they build.

One perspective from which to view measures of effectiveness for CIOs is to look at what the CEO expects from the CIO. All of the experts agreed that the CEO expects the same qualities from a CIO as he does from any other executive. CEOs want CIOs that have business knowledge and experience, executive presence and skills, communications

abilities, technical knowledge, and leadership with a track record of getting things done (Skinner, 1997). All the experts agreed that the CEO wants someone who looks and acts like him and who could potentially take his job. Experts say CIOs should have qualities such as a sense of timing, versatility, a can-do positive attitude, social skills, and intelligence. MOEs for these competencies include staying within budget, the CEO's perception of the CIO's contribution to the business, the CIO's contribution to the executive team, and customer satisfaction (Skinner, 1997). The CEO wants his CIO to become more customer oriented and to focus on business problems, not technology (Keever, 1997). The CEO wants the CIO to bring value to the executive table and possess the skills necessary to become a CEO (Ummel, 1997).

### **3. Potential Measures of Effectiveness of a Navy Medical Chief Information Officer**

#### ***a. Introduction***

From the discussion above, the civilian sector seems to have few quantifiable measures of effectiveness for their CIOs. Many of the measures of effectiveness come from subjective measurements made by the CEO and fellow executives based on personal experience and inclination and user satisfaction. This thesis identifies potential measures of effectiveness for Navy medical CIOs based on the core competencies defined earlier. Those core competencies are leadership competence, communications competence, technological competence, management competence, change management competence, DOD health care business competence, political

competence, and systems thinking competence. Users of information systems are the best source of the effectiveness of the IS department and the CIO. Their input is invaluable in the search for good MOEs.

***b. Leadership Competence Measures of Effectiveness***

The leadership competence involves developing a vision, goals and strategic plan aligned with the organization strategic plan and then selling and implementing the plan. MOEs for the leadership competence include evaluating the CIO plan, then measuring how well the IT strategic plan aligns with the business plan, and how well it is being implemented. A well-written strategic plan will contain a detailed schedule of activities utilizing resources in the attainment of strategic goals and objectives that are based on quantifiable performance measures (Frenzel, 1992). A well-aligned IT strategic plan in the Navy medical environment focuses IT planning on the hospital's mission, goals, and objectives (Dowling, 1987).

Whether or not a CIO develops a plan is a yes or no question, therefore easy to measure. The absence of a strategic plan indicates that the CIO has not attained leadership competence. The presence of a well written and detailed strategic plan that includes a schedule of resource allocations is a MOE of leadership competence. How well the IT strategic plan adequately addresses the hospital's mission, goals and objectives with quantifiable performance measures is an MOE for the strategic alignment portion of the leadership competence. The CIO can poll the CO and ESC members to determine their perception of how well the IT strategic plan aligns with the hospital's strategic plan.

Performance measures of the plan provide another MOE for the Navy medical CIO. They can be tracked over time and a comparison of the planned to actual performance measures can be achieved. Finally a well-developed strategic plan will have some time sensitive milestones attached to it. Measurements of when the time sensitive milestones occur, compared to when they were scheduled to occur, are MOEs for the leadership competence.

*c. Communication Competence Measures of Effectiveness*

The communication competence concerns how well the CIO conveys information concerning IT issues to the organization. One of the CIO's responsibilities is to raise IT literacy and competency within the organization. A MOE for the communications competence asks users to define a particular topic and compare the users' definition with the CIO's definition. For example, if the CIO spends time explaining the client/server environment to the ESC, he provides a practical business application exercise to the members at the end of the meeting. The exercise would provide an opportunity for each executive to state in his own words how the client/server environment operates and what its chief characteristics are. This practice would have three beneficial results:

- It helps the CIO cement the concepts of client/server in the minds of the executives.
- If the executives know they will participate in an exercise, their desire to appear intelligent and attentive to the respondent will increase their attention.

- The CIO will get a good idea back from the executives as to his communication competence.

*d. Technological Competence Measures of Effectiveness*

Technological competence has a number of MOEs already associated with it. Such things as system down time and system recovery time are well-established MOEs. One of the skills of technological competence is technology integration. As new technologies are added to the environment, user surveys can measure user perceptions of how well the IS department did the integration. Three of the key technological competence requirements are to create an agile IT infrastructure, accurate, high quality data, and IS staff expertise essential in the medical environment. User surveys can provide the Navy medical CIO with a MOE of his technological competence.

*e. Management Competence Measures of Effectiveness*

All three aspects of management competence are amenable to MOEs. Financial management already has the MOE of the percentage over budget that many people use to measure a CIO's effectiveness. This MOE measures the ability to budget, not effectiveness of IT support. The Navy medical CIO should be using skills like capital planning and investment and return on investment where it is applicable in his environment. A measure of effectiveness is to compare projected to actual ROI. The MOE developed in the leadership competence discussion above, concerning tracking performance measures over time, is also an MOE for the management competence.

Since customer awareness and response are part of the management competence of the CIO, user surveys can measure user perception of IS department response time to problems. The IS department can also monitor and measure its actual response time. A comparison of the two measures will provide valuable information to the CIO.

Another part of management competence deals with staff and organizational development. Customer surveys can measure the benefit of classes taught by IS staff to users, on issues such as application software. The IS department can develop tests to measure the actual development of staff members that occurs following their attendance at seminars or continuing educational classes. A simple forum where staff who have attended government paid seminars on IS/IT issues share what they have learned with the rest of the staff, could provide the CIO a measure of this competence. The Navy medical CIO or other department members could critique presentations in the forum concerning what the topic added to staff professional development. The IS staff could also develop a report on the educational experience. Staff members would share what the experience contributed to their own development. Finally the CIO could develop tests to measure his staff's development in particular areas the CIO wants to evaluate. By giving the tests over time, the CIO can determine if his staff is maturing.



***f. Change Management and Systems Thinking Measures of Effectiveness***

Change management competence involves planning and managing change and its consequences for the organization and its people. It involves the challenge of planning and managing change while maintaining enough stability to continue to perform the responsibilities of today (Beckhard, 1987). Systems thinking and change management both deal with understanding interrelationships in large systems. Changes occur frequently in Navy medical and IS department environments. After any change, such as a software change, the department can survey users to gauge their concept of how well the change was planned and implemented. Over time a trend of increase or decrease in user satisfaction will develop. This trend will measure both change management and systems thinking competence.

***g. Department of Defense Health Care Business Competence Measures of Effectiveness***

The CO and ESC members are best able to measure a CIO's DOD health care business competence. Discussion at the ESC and individual executive meetings with the CIO will give the other members of the group an idea of what the CIO knows about the DOD health care arena. To measure his effectiveness in this competence, the CIO just needs to ask for the CO and ESC member's input. This can come in personal discussion or evaluation. One management evaluation process involves a manager asking his immediate supervisor, his peers and his subordinates for input on his management.

Adding DOD health care business competence to this type of management evaluation process would provide a valuable MOE. Ultimately the CO will decide if a CIO understands the business. The decision will appear in the CIO's fitness report and in personal discussions.

*h. Political Competence Measures of Effectiveness*

Political competence is more difficult to measure. It could be measured by determining if a Navy medical CIO has power and influence greater than his rank or position in the organization. As in the case of measuring the DOD health care business competence, the CO and ESC will make this determination.

**4. Use of Measures of Effectiveness of a Navy Medical Chief Information Officer**

The author suggests that the measures of effectiveness developed for this thesis be used by the Navy medical CIO to determine his effectiveness. Any use of these MOEs outside this personal use by the Navy medical CIO was not intended by this study. MOEs used to determine a Navy medical CIO's effectiveness must be developed by that manager based on needs and environment. It remains for those in positions of power to determine what measures of effectiveness they wish to use in the evaluation of their employees.

## **V. CONCLUSIONS AND RECOMMENDATIONS**

### **A. CRITICAL SUCCESS FACTORS AND CORE COMPETENCIES**

Critical success factors come from the structure of a particular industry, an organization itself, the environment, and temporal or time-dependent factors. Critical success factors can define a CIO's essential conditions for success. As such they become a set of key job responsibilities of the CIO. Examining CIO critical success factors leads to a determination of a set of core competencies. By monitoring success at meeting core competencies, a CIO's effectiveness in the executive management of his organization can be judged.

The critical success factors this thesis developed for a civilian medical CIO are:

- align the IS function and activities with the organization's strategies;
- strengthen the role of CIO in the organization;
- create, alter and manage the composition and characteristics of IT assets;
- make clinical information systems more useful and relevant to clinicians;
- facilitate the transition to an Integrated Delivery Network;
- develop methods to handle security, privacy and confidentiality concerns.

Core competencies necessary for a civilian medical CIO to be successful at meeting the critical success factors are technical competence, health care business competence, management competence, leadership competence, systems thinking competence, communication competence, and change management competence.

The six critical success factors developed for the DON CIO are:

- develop and sell a strategic plan;
- implement an information technology architecture that supports the strategic plan;
- set goals for information technology within the Department of the Navy;
- manage and establish credibility for information resource management within Department of the Navy;
- increase the technological maturity of the Department of the Navy;
- participate and guide the Chief Information Officer council.

Core competencies necessary for a DON CIO to be successful at meeting the critical success factors are political competence, DOD business competence, communications competence, management competence, technological competence, leadership competence, and change management competence.

Core competencies of a civilian CIO and the Navy medical CIO appear remarkably similar. This could mean that all CIOs, regardless of where they work, will have similar core competencies. It may mean that the responsibilities of the position of CIO define the competencies, rather than the industry or the organization defining the competencies. The list of core competencies for a Navy medical CIO includes leadership competence, communications competence, technological competence, management competence, change management competence, DOD health care business competence, political

competence, and systems thinking competence. All of these competencies must be present if the Navy medical CIO is to be successful.

The critical success factor methodology worked well to define the core competencies of a civilian medical CIO and the core competencies of a DON CIO. The Navy medical CIO's responses to the author's survey, validated the list of core competencies developed by the author through the critical success factor methodology. None of the topics rejected as core competencies appeared in the list of core competencies developed in the critical success factor model.

## **B. MEASURES OF EFFECTIVENESS**

The author developed several measures of effectiveness for a Navy medical CIO to measure his effectiveness in the executive management of the organization. The list of core competencies of a Navy medical CIO provided the basis to develop MOEs. Since the users of information systems are the best source of the effectiveness of the IS department and the CIO, their input is invaluable in the search for good MOEs. The opinions of the users of the CIO's services provide a basis for the CIO to measure his personal effectiveness. Measures of effectiveness for the leadership competence include identifying if the CIO developed a plan, then measuring how well the IT strategic plan aligns with the business plan, and how well it is being implemented. Another MOE for leadership competence and also management competence is created by comparing planned to actual performance measure results.

A MOE for the communications competence asks users to define a particular topic and compare the users' definition with the CIOs definition. Technological competence has a number of MOEs already associated with it. Such things as system down time and system recovery time are well-established MOEs. User surveys can measure user perception of how well the IS department does system integration. User surveys can also measure the user's perception of how agile the IT infrastructure is, if data is accurate and of high quality data, and IS staff expertise. The responses from the user surveys become MOEs for the technological competence.

Management competence provides several MOEs. The financial aspect of management competence already has the MOE of the percentage over budget that many people use to measure a CIO's effectiveness. A new measure of effectiveness is to compare projected to actual ROI. Since customer awareness and response are part of the management competence of the CIO, user surveys can measure user perception of issues such as IS department response time to problems. By comparing IS department measured response time to user perception response time the CIO can gain valuable insight into his management of the IS department. Customer surveys can measure the benefit of classes taught by IS staff to users. The department can develop tests to measure the actual development of staff after they attend seminars or continuing educational classes by requiring staff to brief the rest of the department after they attend a seminar. The Navy medical CIO or other department members could critique the presentation on what the topic added to the staff professional development. Also, the CIO could develop tests to

measure his staff's development in particular areas. By giving the tests over time, the CIO can determine if his staff is maturing.

An MOE developed for measuring the change management competence and the system's thinking competence is to query users concerning their opinion on how well changes are planned and implemented. Trending these surveys will give the CIO a measurement of his change management and systems thinking competence. Through discussions and other interactions the CIO can determine his level of political competence and DOD health care business competence. The MOEs will come by asking for input from his superiors and ESC members. Also a Navy medical CIO will receive a MOE every six months as a mid-year review or an officer's yearly fitness report.

Will developing and using these measures of effectiveness have a positive impact on the Navy medical CIO? A future study could entail enlisting the aid of a group of CIOs to use the MOEs. CIOs would then be asked if MOEs improved their effectiveness in the executive management of the organization. Their opinion could be compared to their future promotion results or another measure of effectiveness.

## **C. RECOMMENDATIONS**

### **1. Navy Medical Department Recommendation**

In the Navy medical department, as in most organizations, the Commanding Officer and Executive Steering Committee establish the enterprise wide direction for the organization including the organization's acceptance and use of technology. The

executive team can agree that information technology is an enabler in solving business problems or that information technology is an expense to be tightly controlled. The executive team molds the corporate culture. Corporate culture must support the innovative application of information technology in order for the organization to get a strategic advantage from information technology and for the CIO to work effectively. A successful CIO must be able to communicate the added value of information technology directly to the executive team.

Research has consistently indicated that membership on the executive board, rather than reporting structure, is the critical indicator of a successful CIO (Earl, 1994). Research has shown no evidence that CIOs higher up in the organizational chart perform better than those lower down but successful CIOs find a way to build relationships with top executives (Earl, 1994) (Koch, 1996). Rank is not the issue, relationships are. The key to the CIO becoming an active member of the executive team is for the CIO to develop an excellent working relationship with the CO and the organization's senior management team. Participation at executive meetings gives the CIO enhanced access to fellow executives, increases the number and quality of relationship-building opportunities and provides the CIO a new level of understanding of the business. More than having a seat at the table, the CIO must be an active member of the executive team. The CIO does this by building strong executive relationships with peers based on his ability to educate and communicate the world of information technology to other team members.



The research is clear; the CIO must have a seat at the executive table if the organization is to take strategic advantage of information technology. It was evident from the results of the survey conducted for this thesis, that many of the personnel currently holding the titles of Navy medical CIOs do not have the reporting level necessary to match the normal definition of Chief Information Officer. While all reported that they had high responsibility for technology at their command, only fifty percent had either high direct reporting levels or representation on the command's senior leadership committee.

Only half of the Navy medical CIOs are in a position to be successful CIOs. If the Navy medical department is going to take full advantage of the Navy medical CIOs' skills in the information age, some way has to be found to have the Navy medical CIO represented on their Command's senior leadership committee. Since the majority of Navy medical CIOs are junior officers, the rank system will not help this objective. An effort to include the Navy medical CIO on the ESC, even if only as an in-house consultant on information technology issues initially, would be a great first step to insure the knowledge and skills of the Navy medical CIO are used to their fullest and the Navy medical department can take full advantage of information technology as a strategic DOD business weapon.

## **2. Educational Program Recommendation**

As the concept espoused by Dr. Langston in the introduction of this thesis, the creation of CIO positions at the command level, begins to occur, there will be a need to develop educational programs to ensure that Department of the Navy CIOs are trained

effectively. Using the critical success factor methodology to determine a set of core competencies for DON CIOs could be used as a basis for the Naval Postgraduate School to build a CIO program. Naval Postgraduate School already has many of the required disciplines necessary to produce such a program. One of the goals of the Information Technology Management curriculum at the Naval Postgraduate School could be to produce DON CIOs. This currently is not the case. Use of this or a similar methodology would tailor a program to meet the needs of future CIOs at many levels in the DOD. Another alternative, to provide the needed education for future command level CIOs, is to use or expand the CIO certification course at the Information Resources Management College. Whatever method is used, some formal program is needed to ensure that the educational requirements of future DON CIOs are met. Meeting these educational requirements will also help ensure that future leaders of the United States Navy will be able to take strategic advantage of information technology thus ensuring the future success of the United States Navy in the information age.

## **APPENDIX A. STEPS FOR MEASURING DOD IT PERFORMANCE**

This section briefly highlights the generic steps for measuring the IM/IT performance of an organization, program, or project.

### ***Step 1 Define mission, key result areas, and business functions***

- Why does the organization exist? (MISSION)
- What major programs are performed by the organization?
- What work effort(s) support major programs?
- What are specific RESULTS produced/delivered by each work effort?
- Who are its customers?
- What are customer and provider expectations?
- What are core competencies?

### ***Step 2 Develop mission related goals***

- Are there standards/goals associated with the mission ?
- Are historic data available upon which to base goals?
- Are data accurate and reliable?
- Are performance goals realistic?
- Do performance goals represent increased efficiency and effectiveness?
- Will performance goals yield improvement in one or more Key Result Areas?
- How can we identify and adapt the best practices to improve organizational performance (i.e., benchmarking)?
- How does the approach compare to best practices in the industry?

### ***Step 3 Generate performance measures***

- What is our product/service?
- Is it measurable?
- What unit/scale of measure is appropriate?
- Which measurable criteria have meaning to whom?
- What is the performance measurement (units & equations)?
- What Key Result Area does the performance measure characterize?

#### ***Step 4 Validate and verify performance measures***

- Does the measure provide useful and important information on the program that justifies the difficulties in collecting, analyzing or presenting the data?
- Does the measure address the aspect of concern? Can changes in the value of the measure be clearly interpreted as desirable or undesirable? Is there a sound, logical basis for believing that the program can have an impact on the measure?
- Does the information provided by the measure duplicate or overlap with information provided by another measure?
- Are likely data sources sufficiently reliable or are there biases, exaggerations, omissions, or errors that are likely to make the measure inaccurate or misleading?
- Can data be collected and analyzed in time for the decision?
- Are there concerns for privacy or confidentiality that would prevent analysts from obtaining the required information?
- Can the resource or cost requirements for data collection be met?
- Does the final set of measures cover the major concerns?
- Are we measuring the right things?

#### ***Step 5 Implement the performance measures and collect data***

- Is the data accessible across tiers?
- Are we prepared to manage cultural change within the organization?

#### ***Step 6 Monitor and assess the results and repeat the process as needed***

- Can we measure better because of our analyzed results?
- How can we improve our business processes?
- How should goals be used to improve resource efficiency and customer deliverables?
- Are current Key Results Areas adequate?
- What recommendations should be forwarded to or acted upon by appropriate tiers. (Paige, 1997b)

## **APPENDIX B. NAVY MEDICAL CHIEF INFORMATION OFFICER SURVEY**

June 16, 1997

Dear Navy Medical CIO Conference Attendee,

Hello! My name is LCDR Tom Moszkowicz. I am a Medical Service Corp officer currently attending Naval Postgraduate School working on my Master of Science in Information Technology Management. My thesis project involves establishing a set of core competencies, skills and measures of effectiveness (MOE's) for Navy Medical Department Chief Information Officers (CIOs) in an attempt to determine what a medical CIO in a Navy environment contributes to the executive management of the organization. All of you have been invited to this meeting because you are Navy Medical CIOs, have many of the job responsibilities, possibly without the title, or have the potential to become Navy Medical CIOs. You are out in the field doing much of this work. My research thus far has been limited to literature reviews. The input of people like you on the front lines is very valuable to my research. I hope you will take the time to answer this short questionnaire. Later in the week, I would also like to take a little of your time to interview you concerning your view of what MOE's are currently being used to evaluate Navy Medical CIO's and your view of what MOE's could or should be used to evaluate the effectiveness of Navy Medical CIO's.

Please feel free to ask any questions concerning any part of this survey and thanks for your help.

Sincerely

Thomas E. Moszkowicz  
LCDR MSC USNR

## Navy Medical Chief Information Officer Survey

### Demographics

Name \_\_\_\_\_ Rank(military or civilian) \_\_\_\_\_  
Age \_\_\_\_\_ Sex \_\_\_\_\_ Years of IS/IT experience \_\_\_\_\_ Years of DOD IS/IT experience \_\_\_\_\_  
If Military - Number of years of active service \_\_\_\_\_ E-Mail Address \_\_\_\_\_  
Command \_\_\_\_\_ Job Title \_\_\_\_\_

### CIO Identification

1. Are you the senior IS/IT professional on staff? Yes \_\_\_\_\_ No \_\_\_\_\_
2. If military are you the senior military IS/IT professional on staff? Yes \_\_\_\_\_ No \_\_\_\_\_
3. Do you have the title of CIO? Yes \_\_\_\_\_ No \_\_\_\_\_

**If you answered yes to number 3, please answer numbers 4 and 5. If you answered no to number 3, please skip to numbers 6, 7 and 8.**

4. Who do you report to in your chain of command? (Check one)  
CO \_\_\_\_\_ XO \_\_\_\_\_ Comptroller \_\_\_\_\_ Director for Administration \_\_\_\_\_ Other (Please Specify) \_\_\_\_\_

5. Are you a member of your command's Executive Steering Committee or senior leadership committee? Yes \_\_\_\_\_ No \_\_\_\_\_

**Please skip to number 9.**

6. Does the senior IS/IT professional at your command have the title of CIO? Yes \_\_\_\_\_ No \_\_\_\_\_

7. Who does the senior IS/IT professional report to in your chain of command? (Check one)  
CO \_\_\_\_\_ XO \_\_\_\_\_ Comptroller \_\_\_\_\_ Director for Administration \_\_\_\_\_ Don't Know \_\_\_\_\_  
Other (Please Specify) \_\_\_\_\_

8. Is the senior IS/IT professional a member of your command's Executive Steering Committee or senior leadership committee? Yes \_\_\_\_\_ No \_\_\_\_\_

**Please continue with number 9.**

9. What percentage of your commands total budget does IS/IT represent?  
\_\_\_\_\_ % If you don't know please check here \_\_\_\_\_

For number 10-13, please circle a number corresponding to the scale from high to low. If you are unsure of the answer please leave the scale blank.

10. Within your organization characterize what you feel is your command's senior IS/IT professional's overall level of responsibility for **managing the technology of your organization?**

High		Medium		Low
1	2	3	4	5

11. Within your organization characterize what you feel is your command's senior IS/IT professional's overall level of responsibility for **managing your organization's technological development?**

High		Medium		Low
1	2	3	4	5

12. Within your organization characterize what you feel is your command's senior IS/IT professional's overall level of responsibility for **maintenance and operations of IT systems?**

High		Medium		Low
1	2	3	4	5

13. Within your organization characterize what you feel is your command's senior IS/IT professional's overall level of responsibility for **planning your organizations future IS/IT needs?**

High		Medium		Low
1	2	3	4	5

## Identification of Core Competencies

*What is a Core Competency (CC)?* Listed below are CC areas that various authors have deemed essential for CIOs to possess if CIOs are to be considered as effective members of the executive team. If a CIO does not have this area of proficiency (CC), he will not be able to be effective as a CIO. A core competency can be contrasted with a skill. The true core competency is essential to be successful; a skill is nice to have but without the skill a person can still succeed as a CIO.

*Your Tasking.* Please circle **yes** if you feel the core competency is one that a Navy Medical CIO must possess to be an effective member of the executive team. Please circle **no** if you do not feel that a particular core competency is essential for a Navy Medical CIO to possess to be an effective member of the executive team. During our future interview I will be asking you if you can identify measures of effectiveness (MOE) that are currently used to measure Navy Medical CIOs in particular competency areas and what MOEs you believe could or should be used to measure Navy Medical CIOs. It is not necessary to have an MOE in mind to mark a core competency as essential for a Navy Medical CIO. Most of the "experts" in this field have not been able to identify MOEs for CIOs. At the end of the list, please add any other CC you feel have not been specified.

Acquisition	Yes No	Organizational Performance	Yes No
Architectural Development	Yes No	Partnership/ Team-building	Yes No
Baseline assessment/ analysis	Yes No	Performance Measurement	Yes No
Benchmarking	Yes No	Planning	Yes No
Best Practices	Yes No	Process Management & Control	Yes No
BPR/Improvement	Yes No	Process Quality Improvement	Yes No
Business Case Analysis	Yes No	Project Management	Yes No
Capacity Planning	Yes No	Research and Development	Yes No
Capital Investment & Planning	Yes No	Results-Based Management	Yes No
Change Management	Yes No	Risk Analysis	Yes No
Computer Standards	Yes No	Risk Management	Yes No
Communication Skills	Yes No	ROI	Yes No
Computer Security	Yes No	SW Development Management	Yes No
Contingency Planning	Yes No	SW Engineering	Yes No
Contracting	Yes No	Source Decision (make vs buy)	Yes No
Cost as an Independent Variable	Yes No	Staff Evaluation	Yes No
Cost/Oper Effectiveness	Yes No	Staff Training and Development	Yes No
Assessment (COEA)	Yes No	Strategic Management & Planning	Yes No
Cost-Benefit Analysis	Yes No	Systems Analysis	Yes No
Customer Awareness	Yes No	Systems Maintenance	Yes No
Facility Planning	Yes No	Technological Competence	Yes No
Functional Economic Analysis	Yes No	Technology Integration	Yes No
Information Resource Management	Yes No	Visionary Focus	Yes No
Investment Management	Yes No	Other _____	
IS Development & Implementation	Yes No	Other _____	
Healthcare Business Knowledge	Yes No	Other _____	
Leadership	Yes No	Other _____	
Life Cycle Management	Yes No	Other _____	
Maturing Technology	Yes No	Other _____	
Modeling & Simulation	Yes No	Other _____	
Organizational Development	Yes No		



# **APPENDIX C. INDIVIDUAL RESULTS OF THE NAVY MEDICAL CHIEF INFORMATION OFFICER SURVEY**

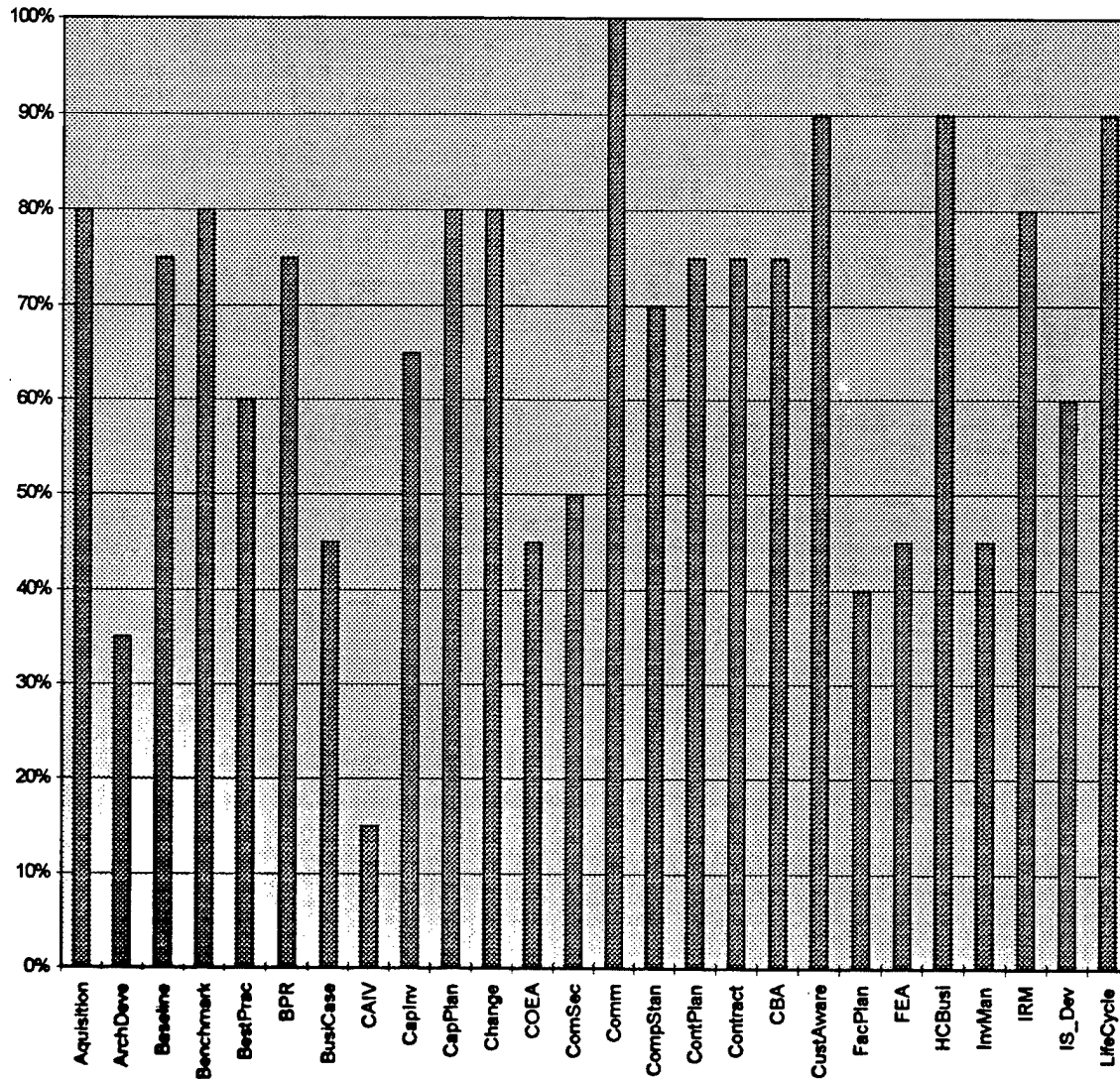
NUMBER	RANK	AGE	SEX	YEAR_IT	YEARS_DD	YRSMIL					
	JOBTITLE	SEN_PRO1	SEN_MIL2	CIO3	BOSS4	ESC5	SR_CIO6				
	BOSS7	ESC8	BUDGET9	TECH10	DEV11	OM12	FUTURE13				
	ACQUIS	ARCH_DEV	BASELINE	BENCHMAR	BESTPRAC	BPR					
	BUSICASE	CAPPLAN	CAP_I_PL	CHANGE	COMPSTAN	COMM					
	COM_SECU	CONTPLAN	CONTRAC	CAIV	COEA	COST_BEN					
	CUSTOME	FACILITY	FEA_IRM	INVEST	IS_DEVHC	BUSIN					
	LEADER	LIFECYCL	MAT_TECH	MOD_SIM	ORG_DEV						
	ORG_PER	PARTNER	PERF_MES	PLANNING	PROC_MAN	PQI					
	PROJ_MAN	ROI_R_D	RESULTS	RISK_ANA	RISK_MAN						
	SW_DEVEL	SW_ENG	SORC_DEC	STAFF_EV	STAFF_TD						
	STRA_MAN	SYS_ANA	SYS_MAIN	TECH_COM	TECH_INT	VISION					
	OTHER1	OTHER2	OTHER3	OTHER4	OTHER5						
1	GS12	46.00	m	10.00	10.00	.00	CIO	y	b	y	1.00
	y	y	1.00	y	15	1.00	1.00	1.00	1.00	n	n
	n	n	n	y	n	n	y	y	y	y	n
	n	n	n	y	y	y	y	n	y	y	n
	y	y	y	n	n	n	y	y	n	y	y
	y	y	y	n	n	y	y	n	n	y	y
	y	y	n	n	y	y	y	consensus forming			
2	O3	37.00	f	7.00	7.00	17.50	"Head, Info Res Man Dept"				y
	y	n	4.00	n	n	4.00	n	#NULL!	1.00	2.00	1.00
	1.00	y	n	n	y	y	n	n	n	y	y
	n	y	n	n	y	n	y	n	y	n	y
	y	y	n	y	y	y	n	n	y	n	y
	n	y	n	y	y	y	n	n	y	n	n
	n	n	n	n	y	n	n	n	y	y	
3	O3	34.00	m	10.00	10.00	15.00	CIO/Head MID	y	y	y	y
	4.00	y	y	4.00	y	1	1.00	1.00	1.00	1.00	y
	n	y	y	n	y	y	y	y	y	y	y
	n	y	y	n	n	y	y	y	b	y	n
	y	y	y	y	n	n	y	y	y	y	y
	y	y	y	y	n	n	y	y	n	n	y
	y	y	y	y	y	n	y	y			
4	O3	33.00	m	8.00	8.00	12.00	"Head, MIS"	y	y	n	n
	4.00	n	n	4.00	n	3	1.00	1.00	1.00	1.00	y
	n	y	y	y	y	n	y	y	y	y	y
	y	y	y	n	n	y	y	n	n	y	y
	y	y	y	y	n	n	y	y	y	y	y
	y	y	y	y	n	n	y	y	y	n	y
	y	y	y	n	y	y	y	y	Marketing		
	Networking										

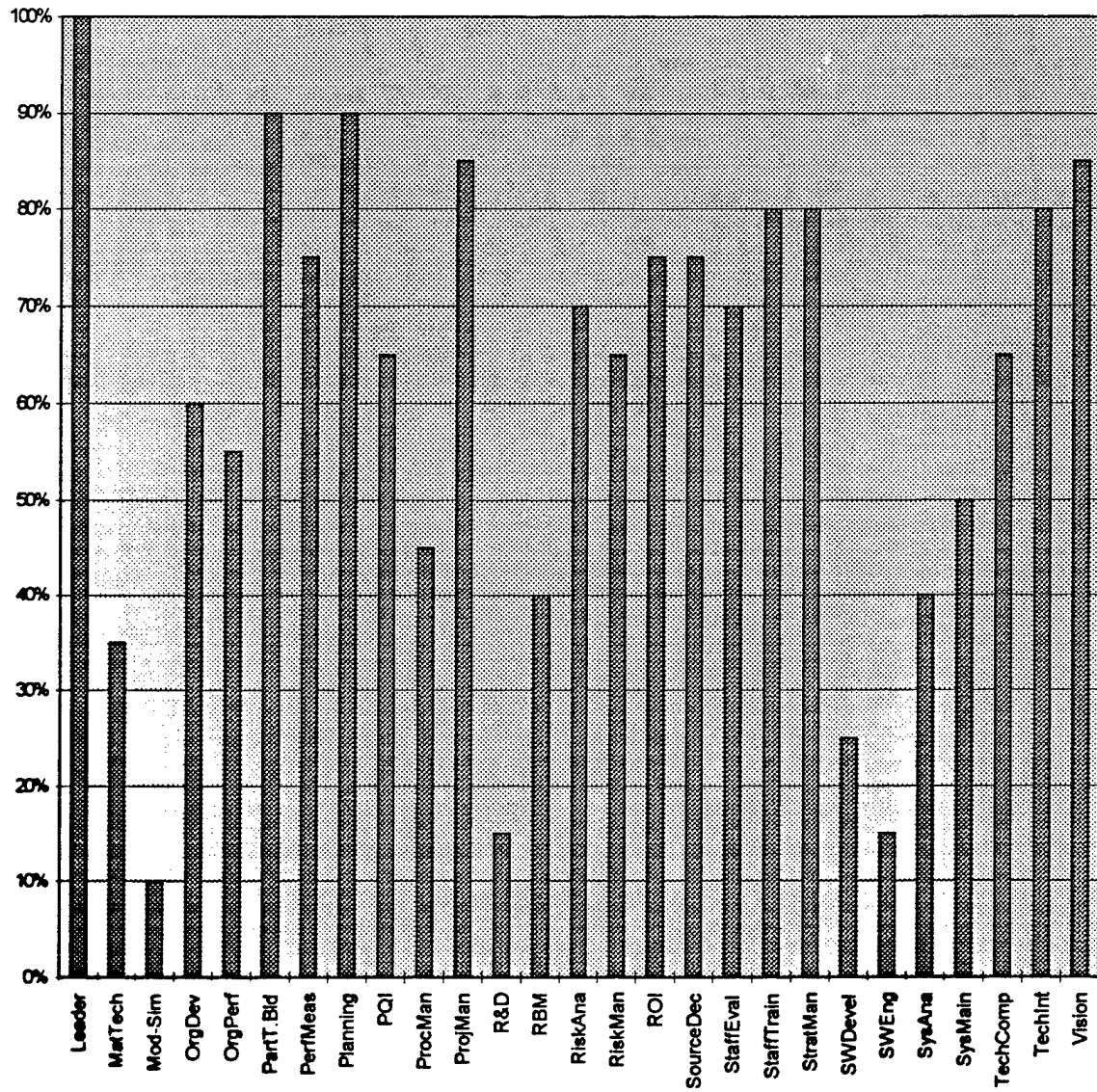
5	O2	33.00	m	4.00	2.00	16.00	CIO	y	y	y	4.00
	n	y	4.00	n	3	2.00	1.00	1.00	1.00	y	y
	y	y	y	y	n	y	y	y	y	y	n
	y	y	n	n	y	y	y	n	y	y	y
	y	y	y	n	n	y	y	y	y	y	b
	b	y	y	n	y	n	n	n	n	y	y
6	O3	39.00	m	17.00	17.00	17.00	CIO	y	y	y	4.00
	y	y	4.00	y	10	1.00	1.00	1.00	1.00	y	y
	y	y	y	y	y	y	y	y	y	y	y
	y	y	n	n	y	y	y	y	y	n	y
	y	y	y	y	n	y	y	y	n	y	n
	n	y	n	y	n	y	n	n	n	y	y
7	O3	38.00	m	9.00	9.00	17.00	CIO/Head MID	y	y	y	y
	4.00	n	y	4.00	n	#NULL!	1.00	1.00	1.00	1.00	y
	n	y	y	y	y	n	y	n	y	y	y
	y	y	y	n	n	y	y	n	n	b	n
	y	y	y	y	y	n	y	n	y	y	y
	y	y	y	y	n	y	n	n	n	n	y
8	O4	38.00	m	14.00	12.00	19.00	CIO	y	y	y	4.00
	n	y	4.00	n	20	2.00	3.00	1.00	1.00	y	n
	y	y	y	y	y	y	y	y	n	y	n
	y	y	n	y	y	y	y	y	y	n	n
	y	y	y	n	n	y	y	y	y	y	n
	y	y	n	n	y	n	y	n	n	y	y
9	O3	35.00	m	4.00	4.00	17.00	Director of Info Sys	y	y	y	y
	n	2.00	y	n	2.00	y	1	1.00	1.00	1.00	1.00
	n	b	y	y	y	y	y	y	y	y	y
	y	y	n	y	y	y	y	y	y	y	y
	y	y	y	y	y	y	y	y	y	y	y
	y	y	y	y	y	y	y	y	y	y	y
10	O4	40.00	m	12.00	12.00	17.00	Head MID	y	y	y	b
	4.00	n	b	4.00	n	#NULL!	1.00	1.00	1.00	1.00	y
	y	y	y	y	b	n	y	y	b	y	y
	y	y	n	n	n	n	y	n	n	y	y
	y	n	y	y	y	n	n	n	y	y	y
	n	y	y	y	n	n	y	y	n	n	n

11	O3	37.00	f	18.00	18.00	14.00	CIO/Head MID	y	y	y	
	4.00	n	y	4.00	n	#NULL!	1.00	1.00	1.00	1.00	y
	n	y	b	y	y	y	y	y	y	y	y
	y	y	y	n	y	y	n	n	n	y	n
	n	y	y	y	n	n	n	n	y	y	y
	n	n	y	y	n	y	y	y	n	n	y
	n	n	y	y	y	y	y	y			
12	O5	#NULL!	m	20.00	16.00	15.00	CIO	y	y	y	4.00
	y	y	4.00	y	#NULL!	3.00	1.00	5.00	1.00	n	n
	n	n	n	n	n	n	n	y	n	y	n
	n	n	n	n	n	y	n	n	n	n	n
	y	y	n	n	n	n	n	y	n	n	n
	n	n	n	n	n	n	n	n	n	n	n
	y	y	n	n	y	n	y				
13	O3	30.00	f	5.00	5.00	9.00	Student	n	n	n	6.00
	n	n	1.00	y	#NULL!	1.00	1.00	3.00	1.00	y	y
	y	y	n	y	n	y	y	y	y	y	y
	y	y	y	y	y	y	y	y	y	y	y
	y	y	y	y	n	y	y	y	y	y	y
	y	y	y	n	y	y	y	y	y	y	y
	y	y	n	y	y	y	y				
14	O4	37.00	m	14.00	14.00	14.00	"Dir, Info Tech Serv"			n	n
	n	2.00	y	y	7.00	y	100	1.00	3.00	4.00	1.00
	y	n	y	y	y	y	y	y	n	y	n
	y	n	y	n	n	y	y	y	n	y	y
	n	y	y	y	y	n	n	y	y	y	y
	y	y	y	y	y	n	y	y	y	n	n
	y	y	y	y	n	y	n	n	y		
15	GS12	52.00	m	20.00	20.00	.00	Director	y	b	n	5.00
	n	n	5.00	y	10	1.00	2.00	1.00	1.00	y	y
	y	n	n	n	n	y	n	n	y	y	y
	y	y	n	n	y	n	n	n	y	n	y
	n	y	y	n	n	n	n	y	y	y	n
	n	y	n	n	n	y	n	n	n	y	n
	y	n	y	n	n	y	n				
16	O3	36.00	m	18.00	18.00	18.00	"Head, IT Ops & Support"	n			n
	n	6.00	b	y	7.00	b	#NULL!	1.00	1.00	1.00	1.00
	y	n	n	y	n	y	y	y	n	y	y
	y	n	y	y	n	y	y	y	n	y	n
	y	n	y	y	y	y	n	n	n	y	y
	y	n	y	y	y	n	n	y	y	y	n
	y	n	n	y	n	n	n	y	y		

17	O3	37.00	f	7.00	7.00	19.00	"Head, Func. Rqrmts"			n	n
	n	6.00	b	n	1.00	y	90	2.00	1.00	2.00	1.00
	y	n	n	y	n	n	n	n	n	n	n
	y	n	n	y	n	n	n	y	n	n	n
	n	n	y	y	y	n	n	n	n	n	y
	y	n	n	n	y	n	n	n	n	n	n
	n	n	n	n	n	n	n	n	n		
18	O3	40.00	f	8.00	8.00	8.00	"Acting Dept Dir, Univ IS"				y
	y	n	5.00	n	n	5.00	y	#NULL!	1.00	1.00	1.00
	1.00	y	y	y	y	y	y	y	y	y	y
	y	y	y	y	y	b	b	y	y	n	y
	y	n	y	y	y	y	n	n	y	y	y
	y	y	y	y	y	y	y	b	y	y	y
	y	y	y	y	n	y	y	y	y	y	
19	O3	33.00	m	5.00	5.00	9.00	Student	n	n	n	5.00
	n	n	6.00	b	#NULL!	1.00	1.00	2.00	1.00	n	n
	y	y	n	y	n	y	n	n	n	y	n
	y	n	n	y	n	y	n	n	y	n	n
	y	y	n	n	n	n	n	n	n	n	n
	n	n	n	n	n	n	y	n	n	n	y
	y	n	n	n	y	n	n	Education of Sr. Mngt			
20	O3	38.00	m	5.00	5.00	17.00	Readiness		n	n	n
	6.00	n	y	7.00	y	110	3.00	2.00	3.00	1.00	y
	y	y	y	y	y	y	y	y	y	y	y
	y	y	y	y	b	y	y	y	y	y	y
	y	y	y	y	y	y	y	y	y	y	y
	y	y	y	y	n	y	y	y	n	n	y
	y	y	y	n	n	n	y	y			

# **APPENDIX D. PERCENTAGE OF RESPONDENTS WHO SELECTED EACH TOPIC AS A CORE COMPETENCY**





## **APPENDIX E. SENGE'S LAWS OF THE FIFTH DISCIPLINE**

1. Today's problems come from yesterday's "solutions."
2. The harder you push, the harder the system pushes back.
3. Behavior grows better before it grows worse.
4. The easy way out usually leads back in.
5. The cure can be worse than the disease.
6. Faster is slower.
7. Cause and effect are not closely related in time and space.
8. Small changes can produce big events - but the areas of highest leverage are often the least obvious.
9. You can have your cake and eat it too - but not at once.
10. Dividing an elephant in half does not produce two small elephants.
11. There is no blame. (Senge, 1990)





## LIST OF REFERENCES

- Anderson, J.G., "Clearing the Way for Physicians' Use of Clinical Information Systems", *Communications of the ACM*, August 1997.
- Appleby, C., "Organized Chaos", *Hospitals and Health Networks*, July 20, 1997.
- Bauer, C. J., "Surveying the Changing Landscape", *Government Executive*, November, 1996.
- Beckhard, R., & Harris, R.T., *Organizational Transitions: Managing Complex Change*, Addison-Wesley, 1987.
- Bennis, W., "The Leadership Crisis", *Executive Excellence*, July 1996.
- Bergman, R., "Health Care In A Wired World", *Hospitals and Health Networks*, August 20, 1994.
- Boyle, R., "Critical Success Factors For Establishing and Maintaining the Position of Chief Information Officer", Joseph A Sellinger School of Business and Management, Loyola College, February, 1993. Available at URL <http://lattanze.loyola.edu/lattanze/research/wp0293.013.html>
- Bresnahan, J., "Mission Possible", *CIO Magazine*, October 15, 1996.
- Burbridge, J. & Boyle, R., "A Contingency-Based Approach to Assessing the Concept of the Chief Information Officer," Joseph A Sellinger School of Business and Management, Loyola College, November 11, 1994. Available at URL <http://lattanze.loyola.edu/lattanze/research/wp0489.002.html>
- CHIME, College of Healthcare Information Management Executives web site, May 1997. Available at URL <http://www.chime-net.org/low>
- Clinton, W. J., "Executive Order 13011 - Federal Information Technology", July 17, 1996. Available at URL <http://www.nismc.navy.mil/don-cio/exord.doc>
- Corbin, L., "Getting a Seat at the Table", *Government Executive*, March, 1997.
- Deagon, B., "Uncle Sam's Tech Projects: They Just Don't Compute", *Investor's Business Daily*, December 4, 1996.

Dowling, A. F., Conference Notes, Navy CIO Conference / CHIME "Information Management Executive Course," Case Western Reserve University, Cleveland, Ohio, June 1997.

Dowling, A. F., "Health Care Information Systems Architecture of the Near Future", *Journal of the Society of Health Systems*, Vol. 1, No. 2, 1989.

Dowling, A.F., "Successful Strategies for Health Care Information Systems Planning", *Software in Healthcare*, April/May, 1987.

Drucker, P., "Not Enough Generals Were Killed!", *Forbes ASAP*, April 8, 1996.

Drucker, P., "The Coming of the New Organization", *Harvard Business Review*, January - February, 1988.

Earl, M.J., "Experiences in Strategic Information Systems Planning", *MIS Quarterly*, March, 1993.

Earl, M.J., & Feeney, D.F., "Is Your CIO Adding Value", *Sloan Management Review*, Spring, 1994.

Emery, J.C., IS4182 Class Notes, "Infrastructure", August, 1997.

Frenzel, C.W., *The Management of Information Technology*, Boyd and Fraser, 1992.

Frew, B., "A Department of the Navy Response to Information Management Reform Legislation: The Cohen Amendment", Naval Postgraduate School Working Paper, October, 1996.

Frew, B., IS4182 Class Notes, "Department of the Navy Chief Information Officer", July, 1997.

Garets, D.E., Conference Notes, Navy CIO Conference / CHIME "Information Management Executive Course," Case Western Reserve University, Cleveland, Ohio, June 1997.

Gartner Group, "CIO Position Description", *CIO Magazine*, November 15, 1996. Available at URL [http://www.cio.com/CIO/rc\\_posit.htm](http://www.cio.com/CIO/rc_posit.htm)

Glaser, J.P., "Beware Return on Investment", *Healthcare Informatics*, June, 1997.

Glaser, J.P., Conference Notes, Navy CIO Conference / CHIME "Information Management Executive Course," Case Western Reserve University, Cleveland, Ohio, June 1997.

Hammer, M., *Beyond Reengineering*, HarperCollins, 1996.

Hoffman, G. M., *The Technology Payoff*, Irwin Professional Publishing, 1994.

IRMC, Information Resource Management College web site, May 1997. Available at URL <http://www.ndu.edu/irmc>

ITMRA, Information Technology Reform Act of 1996, Annotated version, August 8, 1996. Available at URL <http://www.dtic.mil/c3i/cio/itmra.Annot.html>

ITRB, Information Technology Review Board web site, August 5, 1997. Available at URL <http://itrb.fed.gov>

Keever, W. Conference Notes, Navy CIO Conference / CHIME "Information Management Executive Course," Case Western Reserve University, Cleveland, Ohio, June 1997.

Khoury, P.F., & Vogel, D.A., "The New Era of Procurement for Federal Information Technology Resources", *Contract Management*, June, 1997.

Kilman, D.G., & Forslund, D.W., "An International Collaboratory Based on Virtual Patient Records", *Communications of the ACM*, August 1997.

Koch, C., "Sitting in the Hot Seat", *CIO Magazine*, February 15, 1996. Available at URL [http://www.cio.com/CIO/inprintcio\\_021596.html](http://www.cio.com/CIO/inprintcio_021596.html)

Kongstvedt, P. R., *The Managed Health Care Handbook*, Aspen, 1996.

Langston, M., Briefing at the Naval Postgraduate School, Monterey Ca., July 21, 1997a.

Langston, M., DON CIO web site, July, 1997b. Available at URL <http://www.doncio.navy.mil//home.html>

Laudon, Kenneth C. & Laudon, Jane P., *Essential of Management Information Systems*, Prentice Hall, 1995.

Laurent, A., "A Whole New Ball Game", *Government Executive*, September, 1996.

Laurent, A., "Get Wired", *Government Executive*, September, 1996.

- Laurent, A., "Technology Tamers", *Government Executive*, October, 1996.
- Luftman, J.N., "Align in the Sand", *Computerworld*, February 17, 1997.
- MacMillan, I., *Strategy Formulation: Political Concepts*, West, 1976.
- Martin, J., Conference Notes, Navy CIO Conference / CHIME "Information Management Executive Course", Case Western Reserve University, Cleveland, Ohio, June 1997.
- NMIMC, Naval Medical Information Management Center web site, August, 1997.  
Available at URL <http://www-nmimc.med.navy.mil>
- Paige Jr., E., "Clinger-Cohen General Core Competency Areas, March 28, 1997.  
Available at URL <http://www.dtic.mil/c3i/cio/cioedtr2.html>
- Paige Jr., E., "Department of Defense Guide for Managing Information Technology (IT) as an Investment and Measuring Performance", Version 1.0, February 10, 1997. Available at URL <http://www.dtic.mil/c3i/cio/guide.doc>
- Palvia, S., Palvia, P., & Zigli, R., *Global Issues of Information Technology Management*, Idea Group Publishing, 1992.
- Pastore, R., "Survival of the Fittest", *CIO Magazine*, November 1, 1996.
- Porter, K., "New Players Try to Sort Out Who Is Running the IT Show", *Government Computer News*, October 21, 1996.
- Raghupathi, W., "Health Care Information Systems", *Communications of the ACM*, August 1997.
- Rindfleisch, T.C., "Privacy, Information Technology, and Health Care", *Communications of the ACM*, August 1997.
- Rockart, J.F., "Chief Executives Define Their Own Data Needs", *Harvard Business Review*, March - April, 1979.
- Row, H., "The CIO Role - Taking Care of Business," *CIO Magazine*, April 1, 1997.
- Selznick, P., *Leadership in Administration*, Row and Peterson, 1957.
- Senge, P.M., *The Fifth Discipline*, Doubleday/Currency, 1990.

SIM, Society for Information Management web site, May, 1997. Available at URL <http://www.simnet.org>

Skinner, R.I., Conference Notes, Navy CIO Conference / CHIME "Information Management Executive Course," Case Western Reserve University, Cleveland, Ohio, June 1997.

Sprague, R.H. & McNurlin, B.C., *Information Systems Management in Practice*, Prentice Hall, 1993.

Strassman, P., "CIO's: The Chosen Elite?", *Computerworld*, July 4, 1994.

Ummel, S., Conference Notes, Navy CIO Conference / CHIME "Information Management Executive Course," Case Western Reserve University, Cleveland, Ohio, June 1997.

Weisbord, M.R., "Organizational Diagnosis: Six Places To Look for Trouble With or Without a Theory", *Group and University Studies*, December, 1976.



## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center.....2  
8725 John J. Kingham Road., Ste 0944  
Ft. Belvoir, Virginia 22060-6218
  
2. Dudley Knox Library.....2  
Naval Postgraduate School  
411 Dyer Rd.  
Monterey, California 93943-5101
  
3. Commanding Officer, Naval Medical Information Management Command.....1  
8901 Wisconsin Avenue  
Building 27  
Bethesda, Maryland 20889-5605
  
4. Captain James Scaramozzino.....1  
Institute for Defense Education and Analysis  
Naval Postgraduate School  
Monterey, California 93943
  
5. Professor Barry Frew, Code SM/FW.....1  
Department of Systems Management  
Naval Postgraduate School  
Monterey, California 93949
  
6. Dr. Mark Nissen, Code SM/NI.....1  
Department of Systems Management  
Naval Postgraduate School  
Monterey, California 93949
  
7. LCDR Thomas E. Moszkowicz.....1  
59569A Ke Iki Rd  
Haleiwa, Hawaii 96712